TIBCO LogLogic® Compliance Suite - ITIL Edition Guide

Software Release 3.9.0
November 2017
Document Updated: April 2018

Two-Second Advantage®

Important Information

THIS SOFTWARE MAY BE AVAILABLE ON MULTIPLE OPERATING SYSTEMS. HOWEVER, NOT ALL OPERATING SYSTEM PLATFORMS FOR A SPECIFIC SOFTWARE VERSION ARE RELEASED AT THE SAME TIME. SEE THE README FILE FOR THE AVAILABILITY OF THIS SOFTWARE VERSION ON A SPECIFIC OPERATING SYSTEM PLATFORM.

THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT.

THIS DOCUMENT COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN; THESE CHANGES WILL BE INCORPORATED IN NEW EDITIONS OF THIS DOCUMENT. TIBCO SOFTWARE INC. MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE PRODUCT(S) AND/OR THE PROGRAM(S) DESCRIBED IN THIS DOCUMENT AT ANY TIME.

THE CONTENTS OF THIS DOCUMENT MAY BE MODIFIED AND/OR QUALIFIED, DIRECTLY OR INDIRECTLY, BY OTHER DOCUMENTATION WHICH ACCOMPANIES THIS SOFTWARE, INCLUDING BUT NOT LIMITED TO ANY RELEASE NOTES AND "READ ME" FILES.

This document contains excerpted portions of the IT Infrastructure Library® ("ITIL®") framework (collectively, the "Regulatory Language"). The Regulatory Language is provided by TIBCO solely for your convenience and to provide context for certain functionality of the TIBCO LogLogic® products. The inclusion or omission by TIBCO of any Regulatory Language is in no way intended as legal advice regarding the ITIL framework and does not constitute any representation or warranty that any TIBCO products comply with the terms contained in such Regulatory Language. If you have additional questions about the ITIL framework, you should consult with an attorney for further legal guidance.

Contents

Figures

TIBCO Documentation and Support Services

How to Access TIBCO Documentation

Documentation for TIBCO products is available on the TIBCO Product Documentation website, mainly in HTML and PDF formats.

The TIBCO Product Documentation website is updated frequently and is more current than any other documentation included with the product. To access the latest documentation, visit https://docs.tibco.com.

Product-Specific Documentation

The following documents for this product can be found on the TIBCO Documentation site:

- *TIBCO LogLogic® Compliance Suite - ITIL Guide*
- *TIBCO LogLogic® Compliance Suite - ITIL Readme*
- *TIBCO LogLogic® Compliance Suite - ITIL Release Notes*

How to Contact TIBCO Support

You can contact TIBCO Support in the following ways:

- For an overview of TIBCO Support, visit http://www.tibco.com/services/support.
- For accessing the Support Knowledge Base and getting personalized content about products you are interested in, visit the TIBCO Support portal at https://support.tibco.com.
- For creating a Support case, you must have a valid maintenance or support contract with TIBCO. You also need a user name and password to log in to https://support.tibco.com. If you do not have a user name, you can request one by clicking Register on the website.

How to Join TIBCO Community

TIBCO Community is the official channel for TIBCO customers, partners, and employee subject matter experts to share and access their collective experience. TIBCO Community offers access to Q&A forums, product wikis, and best practices. It also offers access to extensions, adapters, solution accelerators, and tools that extend and enable customers to gain full value from TIBCO products. In addition, users can submit and vote on feature requests from within the TIBCO Ideas Portal. For a free registration, go to https://community.tibco.com.

ITIL History

IT Infrastructure Library® (ITIL®) is a process-oriented IT control framework for service management organizations. Developed in the late 1980s by the United Kingdom, this framework has been widely adopted and is now the most accepted and used IT service management best practices approach in the world.

In the late 1980s, the UK recognized that the cost of IT infrastructures must be controlled so they commissioned the Central Computer and Telecommunication Agency (CCTA) to address the issue. This directive resulted in the publication of the Government Information Technology Infrastructure Management, or GITIM. The goal of GITIM was to define a framework that would ensure the efficient and financially responsible use of IT resources within the British government and the private sector. Apparently, GITIM satisfied a need. Governments and private industry in Europe adopted the framework very quickly and soon was proclaimed the world’s “defacto standard” for IT service management. GITIM was ITIL version 1.0.

Today’s ITIL version 3.1 was also developed by the UK government under the Office of Government Commerce (OGC) which merged with the CCTA in 2000. Version two, like its predecessor, concentrated on the service management model but the new publications were more concise and usable.

ITIL’s popularity continues to spread. Microsoft used the ITIL framework to develop the Microsoft Operations Framework (MOF) and the first ITIL-aligned British Standard (BS15000) has been issued. In 2005, the International Standards Organization (ISO) placed BS15000 on the fast track to becoming an ISO standard (ISO20000).

ITIL is divided into a service of 8 publications commonly known as “sets”. The 8 publications are:

- Service Support
- Service Delivery
- Planning to Implement Service Management
- Software Asset Management
- Applications Management
- Service Delivery
- The Business Perspective
- ICT Infrastructure Management

Together these publications describe the processes that are necessary for the effective management of IT organizations. According to ITIL, service management is composed of both service support and service delivery organizations whose working relationship with the customer is specifically defined by a Service Level Agreement (SLA).

The popularity of ITIL and IT and business processes automation is fueled by two concurrent market forces resulting into a “perfect storm” for ITIL and IT Service Management:

- The desire to reduce IT costs while maintaining and improving IT Service Quality
- The requirement to create better control and visibility into IT for regulatory compliance

IT Service Management

IT Service Management (ITSM) is a framework covering two major aspects: Service Support and Service Delivery. It is an integrated approach providing best practice guidelines to IT organizations on how to effectively delivery services to its business customers. ITSM is a set of process-based best practices comprised of processes, people, technology, organization, and integration. ITSM is generally employed to meet unique customer requirements and priorities.

Service Delivery is a set of integrated processes focused on ensuring IT can provide adequate support to the business customers. Service Support is a set of integrated processes to ensure that users have access to the services to support the business functions.

According to ITIL, there's a clear distinction between "Customers" and "Users". Customers are defined as senior management who commissioned and paid for the IT services. Users are defined as people who use the services on a day-to-day basis.

Service Delivery

Service Delivery consists of five disciplines. These are:

- Service Level Management
- Capacity Management
- Contingency Planning
- Availability Management
- IT Financial Management

Service Support

The six Service Support disciplines are:

- Configuration Management
- Problem Management
- Incident Management
- Change Management
- Service / Help Desk
- Release Management

IT Service Validation

Measurement and validation capabilities should be a first priority when considering IT Service Management. Effectively, you cannot manage what you cannot measure and putting in place any proactive management framework, from service level management to capacity planning, is fruitless if you cannot measure what is actually happening in your data center.

Metrics are critical to improving business performance. In order to prove that the ITSM implementations are effective and beneficial to the business, IT must be able to measure and validate the benefits of the ITSM implementation and the process improvements.

The importance of this cannot be overstressed, as inclusion of processes that cannot be effectively monitored almost always result in disputes and eventual loss of faith in the ITSM process. A lot of organizations have discovered this the hard way and as a consequence, have absorbed heavy costs both in financial sense as well as in the terms of negative impacts on their culture.

Metrics can also help to prove the value of ITSM before and after the projects gets approved. The best way to "sell ITIL" to the CIO is to provide concrete examples and figures on how ITSM benefits the organization. For example,

- Cut incident resolution rates by 40%
- Cut network failure downtime by 30%
- Reduce labor waste by 25% (labor waste include time IT personnel has to run around to obtain information necessary to do their job)
- Reduce IT infrastructure cost by 20%

This Best Practices guide will explain how log data can be used effectively to measure and validate the core IT Service Management processes. To ensure success of the ITSM implementations, TIBCO LogLogic has defined the following Service Validation steps based on collecting and analyzing log data that is already available in any data center today:

Assess the current state of the IT services

Monitor the ongoing status of the IT services

Measure the result of the process implementations

Validate the effectiveness and benefits of the process changes

Assess the current state of the IT services

In order to understand the IT services, IT must be able to assess the current state. The current state gives IT organizations a starting point in which to define improvement criteria and design processes to meet those criteria. For example, based on the assessment of the network infrastructure, the IT organization may determine that it needs to reduce the number of network failures by 30%. The assessment allows the IT organization to set specific target metrics and measure against these targets. These targets set the direction for the IT organization.

Monitor the ongoing status of the IT services

To ensure the successful outcome of the process implementations, IT must be able to continuously monitor the IT services to ensure process improvement. Continuous monitoring allows the IT organization to intervene and adjust the processes as needed. If the new processes being implemented to reduce network failures by 30% is not meeting the goals at preset milestones, the IT organization will have the opportunity to review the processes and technologies, and adjust the implementation to ensure the success of the implementation.

Measure the result of the process implementations

What cannot be measured cannot be understood, what cannot be understood cannot be improved. IT must periodically measure the result of the process implementations to ensure improvements are being made. Reporting should be used to show no adverse impacts have been introduced and improvement goals are met. Measuring results early on may also identify “quick wins” that can be used to justify further ITSM implementation projects.

Validate the effectiveness and benefits of the process changes Based on the reports from step 3, IT must validate that the improvements are meeting the set goals. For example, if the original goal is to reduce network failure incidents by 30%, IT must validate that the new processes implemented are indeed meeting this goal.

Conclusions:

Nothing should be included in the IT Service Management process unless it can be effectively measured and validated.

Existing measurement capabilities should be reviewed and upgraded as necessary.

Ideally this should be done ahead of, or in parallel with, the approval of any IT Service Management process.

A universal, economical and effective way to measure core IT Service Management processes and objectives is by collecting and analyzing log data.

TIBCO LogLogic® Compliance Suite - ITIL Edition

The TIBCO LogLogic® Compliance Suite - ITIL Edition delivers automated process validation and includes reporting and alerts that can be used to evidence and enforce business and IT policies related to compliance. By automating compliance reporting and alerting based on critical data collected and stored by TIBCO LogLogic's Appliances, the TIBCO LogLogic® Compliance Suite - ITIL Edition removes the complexity and resource requirements typically needed to implement control frameworks to successfully meet ITL and ITSM and other compliance requirements.

TIBCO LogLogic® Compliance Suite - ITIL Edition:

- Automates compliance activities and dramatically improves audit accuracy.
- Reduces the time to mitigate the risk factor.
- Allows organizations to use infrastructure data to provide evidence of and enforce IT controls.
- Provides industry-leading reporting depth and breadth, including real-time reporting and alerting for ITL and ITSM compliance.
- Delivers approximately 166 out-of-the-box Compliance Reports and 91 out-of-the-box Compliance Alerts.
- Enables customization of any Compliance Report to map specifically to your organization's unique policies and requirements.

Compliance Reports and Alerts Overview

Log data allows organizations to manage the challenge of achieving and maintaining ITL and ITSM compliance. TIBCO LogLogic's compliance reports and alerts generally fall into the following categories:

- Security and Threat Management
- Change and Configuration Management
- Identity and Access Management
- Monitoring and Reporting

Security and Threat Management

The TIBCO LogLogic® Compliance Suite - ITIL Edition includes reports and alerts to show that all network security devices, including firewalls which control traffic into a company's network, as well as intrusion detection systems which monitor the traffic, have been configured appropriately to allow only the requested and approved traffic in and out of the network.

Non-compliance in this area may result in unauthorized access from the Internet. Often, seemingly insignificant paths to and from the Internet can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network and they are featured prominently in the TIBCO LogLogic® Compliance Suite - ITIL Edition.

Change and Configuration Management

The TIBCO LogLogic® Compliance Suite - ITIL Edition includes reports and alerts to show that all system changes are appropriately requested, approved, tested, and validated by authorized personnel prior to implementation in the production environment.

Non-compliance in this area may result in unauthorized changes and/or improper roll-out of new source code to key systems. This may negatively impact the confidentiality, integrity, and availability of information.

Identity and Access Management

The TIBCO LogLogic® Compliance Suite - ITIL Edition includes reports and alerts to show that all ITL and ITSM-related systems (i.e., networks, applications, and databases) are appropriately secured to prevent unauthorized use, disclosure, modification, damage or loss of data, and that the division of roles and responsibilities has been implemented to reduce the possibility for a single individual to subvert a critical process. Management needs to ensure that personnel are performing only authorized duties relevant to their respective jobs and positions.

Non-compliance may result in unauthorized or inappropriate access to key systems, which may negatively impact the confidentiality, integrity, and availability of information.

Monitoring and Reporting

The TIBCO LogLogic® Compliance Suite - ITIL Edition includes reports and alerts to allow customers to continuously monitor the IT infrastructure for security violations and other anomalies. Reports are provided in a format meaningful to stakeholders. The monitoring statistics should be analyzed and acted upon to identify trends for individual systems and the overall ITL and ITSM environment.

Non-compliance in this area could significantly impact service availability as well as security of the IT infrastructure.

TIBCO LogLogic Compliance Suite Setup

Setting up the TIBCO LogLogic® Compliance Suite - ITIL Edition comprises checking that all prerequisites are met before starting the installation process, installing the Compliance Suite file, and enabling the alerts.

See Installing the Compliance Suite and Enabling Compliance Suite Alerts for more details.

Installing the Compliance Suite

Prerequisites

Before installing the TIBCO LogLogic® Compliance Suite - ITIL Edition, ensure that you have:

- TIBCO LogLogic LX or MX or ST Appliance running TIBCO LogLogic Release 5.7.x or higher
- TIBCO LogLogic® Log Source Packages (LSP) 32.1 or 33 installed

The Compliance Suite includes one file containing ITIL filters, custom reports, and alerts.

- `itil.xml` – ITIL and ITSM Reports, Search Filters, and Alerts

> ⚠ If you have previously imported any earlier versions of the Compliance Suite files, importing this version of the Compliance Suite will not overwrite the original files or any changes that have been made, unless you have saved the changes to the object using the default name.
>
> If you have made any changes to base Compliance Suite alerts, search filters, or custom reports, TIBCO recommends saving these items with non-default names. This will help ensure that the latest Compliance Suite updates can be installed without any compatibility issues or naming conflicts.

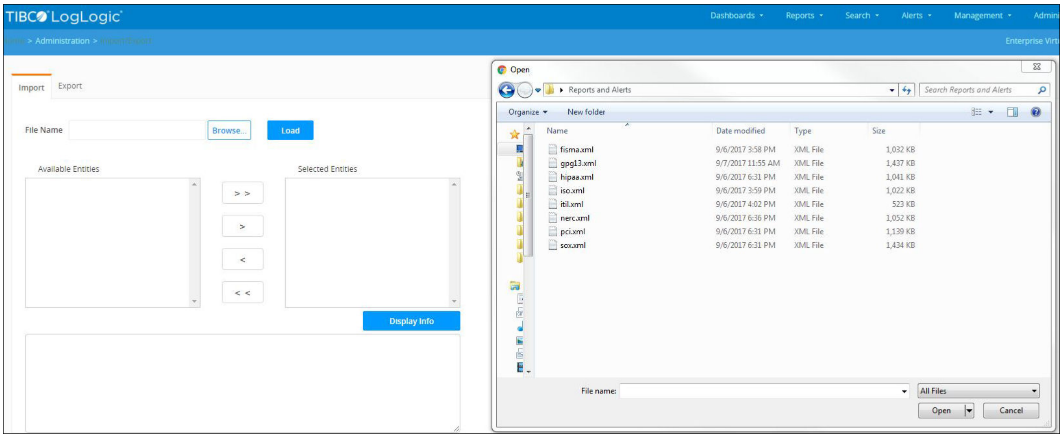
Procedure

1. Log in to your TIBCO LogLogic LX or MX or ST Appliance as admin.
2. From the navigation menu, select **Administration** > **Import or Export** .

   The **Import** and **Export** tabs appear.
3. Load the Compliance Suite file by completing the following steps:
   a) In the **Import** tab, click **Browse**.
   b) In the **File Upload** window, select the appropriate XML file and then click **Open**.

   The following figure shows the **File Upload** window that appears after clicking **Browse** on the **Import** tab.

   Loading a Compliance Suite File



Name	Date modified	Type	Size
fisma.xml	9/6/2017 3:58 PM	XML File	1,032 KB
gpg13.xml	9/7/2017 11:55 AM	XML File	1,437 KB
hipaa.xml	9/6/2017 6:31 PM	XML File	1,041 KB
iso.xml	9/6/2017 3:59 PM	XML File	1,022 KB
itil.xml	9/6/2017 4:02 PM	XML File	523 KB
nerc.xml	9/6/2017 6:36 PM	XML File	1,052 KB
pci.xml	9/6/2017 6:31 PM	XML File	1,139 KB
sox.xml	9/6/2017 6:31 PM	XML File	1,434 KB

c) Click **Load**.

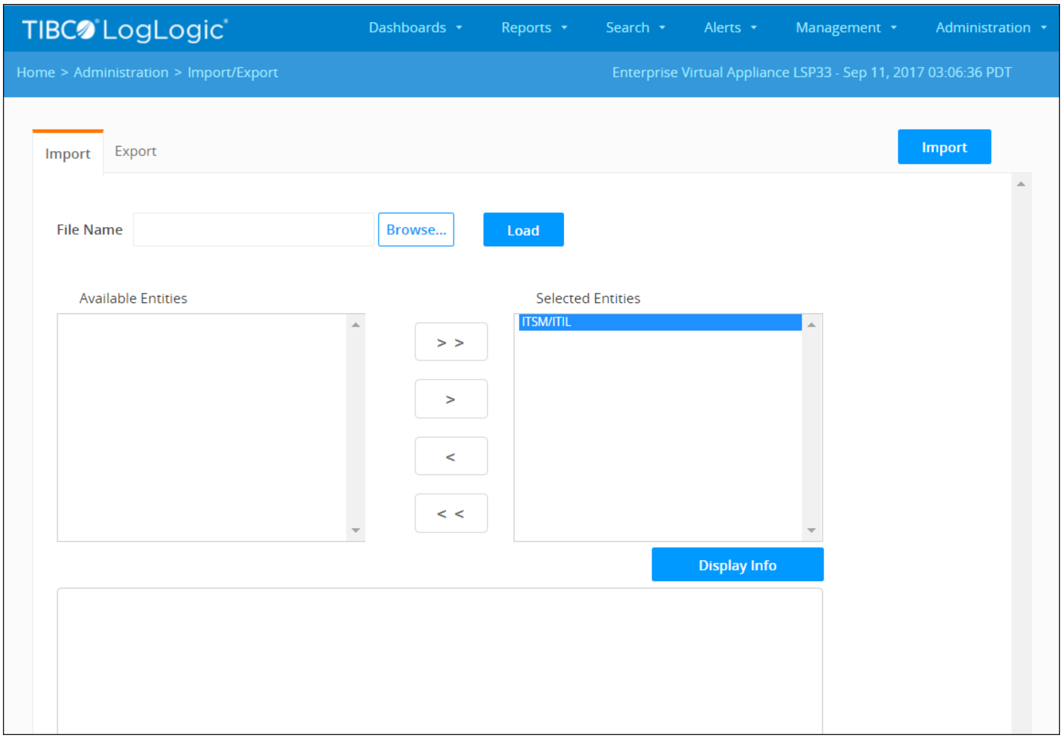
This loads the **Available Entities** from the XML file.

d) Click **Add All Entities**.

> You can also select the specific ITSM/ITIL entity from the **Available Entities** text block, and then click **Add Selected Entities.**

The following figure shows all entities of the ITIL XML file that were selected by clicking **Add All Entities**.

Selected Entities to be Imported



4. Click **Import**.

An import successfully completed message appears above the **File Name** text field.

Installation is complete after the XML file is imported successfully.

The Compliance Suite Usage

Once you have successfully installed the TIBCO LogLogic® Compliance Suite - ITIL Edition, you can begin using the custom reports and alerts.

The following sections help you view, test, and modify, the packaged custom reports and alerts. The custom reports and alerts were designed to run out-of-the box; however, TIBCO LogLogic enables you to perform further customization if necessary.

The Compliance Suite Reports

All TIBCO LogLogic® Compliance Suite - ITIL Edition reports are designed to run out-of-the box as well as to be flexible if you need to make modifications based on your business needs.

For a description of all custom reports in this Compliance Suite, see TIBCO LogLogic Reports for ITIL.

Viewing Compliance Suite Reports and Output Data

Using TIBCO LogLogic LX or MX or ST Appliance, you can view all the Compliance Suite reports for the device and run them as well as view the output data.

Procedure

1. Log in to your TIBCO LogLogic LX or MX or ST Appliance as admin.

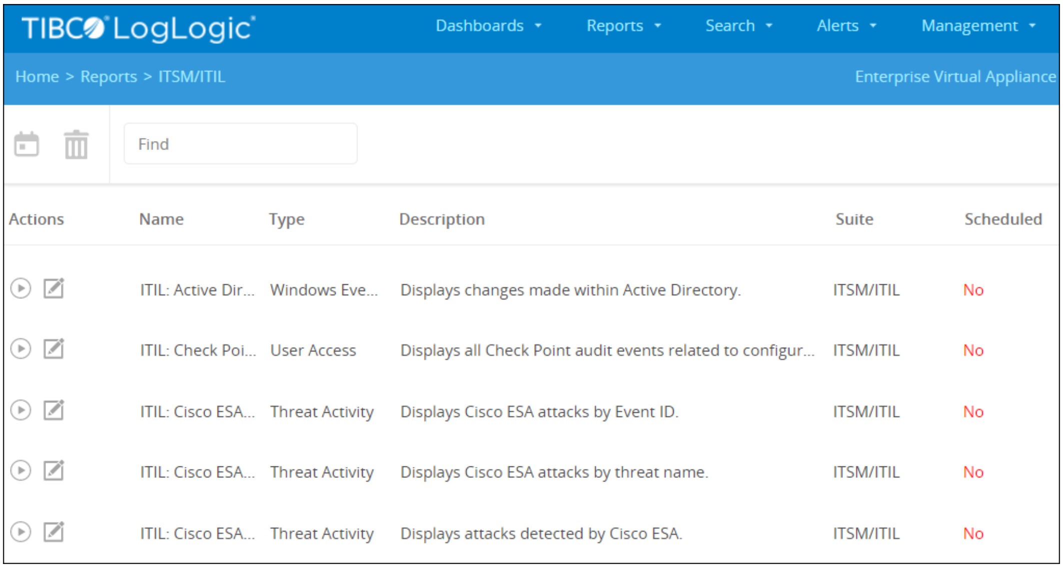
   From the navigation menu, select **Reports** > **ITSM or ITIL** .

2. On the **Reports** page, you can see all of the custom reports you loaded during the installation process.

3. You can navigate through all of the custom reports using the page navigation buttons at the top and bottom of the **Reports** page.

   The following figure shows a cropped list of the Compliance Suite reports loaded from the ITIL XML file.

   Compliance Suite Reports



Actions	Name	Type	Description	Suite	Scheduled
	ITIL: Active Dir...	Windows Eve...	Displays changes made within Active Directory.	ITSM/ITIL	No
	ITIL: Check Poi...	User Access	Displays all Check Point audit events related to configur...	ITSM/ITIL	No
	ITIL: Cisco ESA...	Threat Activity	Displays Cisco ESA attacks by Event ID.	ITSM/ITIL	No
	ITIL: Cisco ESA...	Threat Activity	Displays Cisco ESA attacks by threat name.	ITSM/ITIL	No
	ITIL: Cisco ESA...	Threat Activity	Displays attacks detected by Cisco ESA.	ITSM/ITIL	No

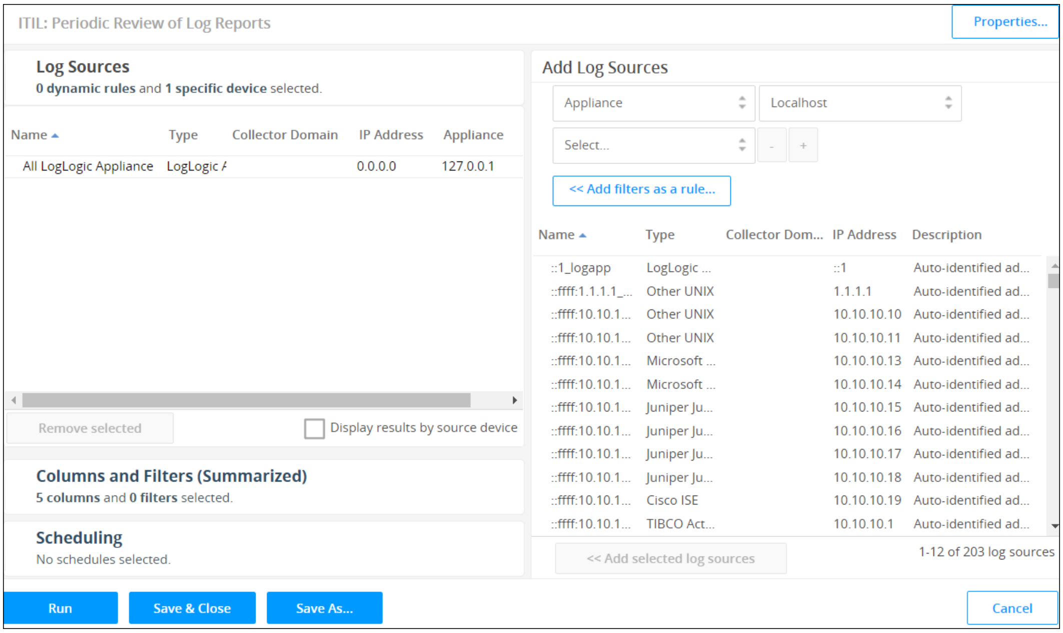
4. Click the **Edit** button to see details such as, the Appliance where the report runs, the associated device type, and when the report runs.

   a) To view the filter parameters, click **Columns and Filters**.

   b) To view details about a report such as the report name and description, click **Properties**.

The following figure shows the details of the **ITIL: Periodic Review of Log Reports** report.

Periodic Review of Log Reports Report Details



ITIL: Periodic Review of Log Reports

Log Sources

0 dynamic rules and **1 specific device** selected.

Name ▲	Type	Collector Domain	IP Address	Appliance
All LogLogic Appliance	LogLogic A		0.0.0.0	127.0.0.1

□ Display results by source device

Columns and Filters (Summarized)

5 columns and **0 filters** selected.

Scheduling

No schedules selected.

Add Log Sources

Appliance | Localhost

Select...

Name ▲	Type	Collector Dom...	IP Address	Description
::1_logapp	LogLogic ...		::1	Auto-identified ad...
::ffff:1.1.1.1_...	Other UNIX		1.1.1.1	Auto-identified ad...
::ffff:10.10.1...	Other UNIX		10.10.10.10	Auto-identified ad...
::ffff:10.10.1...	Other UNIX		10.10.10.11	Auto-identified ad...
::ffff:10.10.1...	Microsoft ...		10.10.10.13	Auto-identified ad...
::ffff:10.10.1...	Microsoft ...		10.10.10.14	Auto-identified ad...
::ffff:10.10.1...	Juniper Ju...		10.10.10.15	Auto-identified ad...
::ffff:10.10.1...	Juniper Ju...		10.10.10.16	Auto-identified ad...
::ffff:10.10.1...	Juniper Ju...		10.10.10.17	Auto-identified ad...
::ffff:10.10.1...	Juniper Ju...		10.10.10.18	Auto-identified ad...
::ffff:10.10.1...	Cisco ISE		10.10.10.19	Auto-identified ad...
::ffff:10.10.1...	TIBCO Act...		10.10.10.1	Auto-identified ad...

1-12 of 203 log sources

5. Run the report to view the report output data by completing the following steps:

   a) Click **Run**.

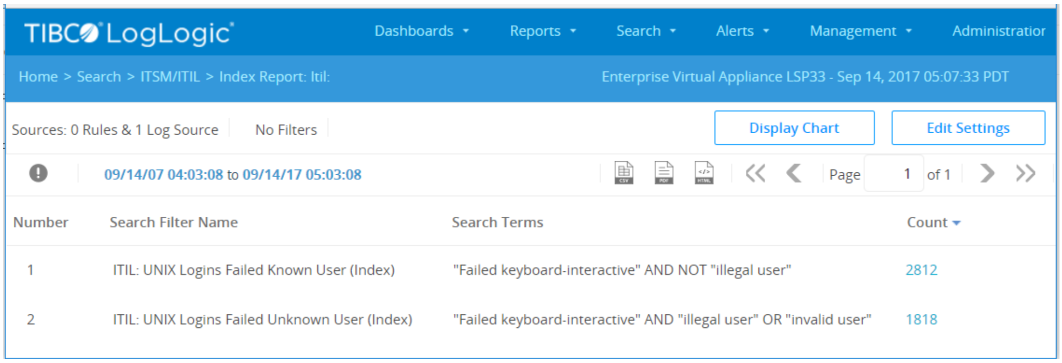
      The report runs and returns data based on the set parameters.

   b) To view detailed drill-down information, click the **Count** link.

> You can use the **Back to summarized results** button to return to the main data output view.

The following figure shows sample results from the **ITIL: Periodic Review of Log Reports** report.

Periodic Review of Log Reports Results



Home > Search > ITSM/ITIL > Index Report: Itil:

Enterprise Virtual Appliance LSP33 - Sep 14, 2017 05:07:33 PDT

Sources: 0 Rules & 1 Log Source | No Filters

09/14/07 04:03:08 to 09/14/17 05:03:08

Page 1 of 1

Number	Search Filter Name	Search Terms	Count ▾
1	ITIL: UNIX Logins Failed Known User (Index)	"Failed keyboard-interactive" AND NOT "illegal user"	2812
2	ITIL: UNIX Logins Failed Unknown User (Index)	"Failed keyboard-interactive" AND "illegal user" OR "invalid user"	1818

> If you want to modify the main data output view, you can modify the report parameters and then run the report again.

Customizing Compliance Suite Reports

The TIBCO LogLogic® Compliance Suite - ITIL Edition reports are designed to run out-of-the-box to meet specific compliance requirements. However, you may want to modify the reports to include additional information or devices depending on your business needs.

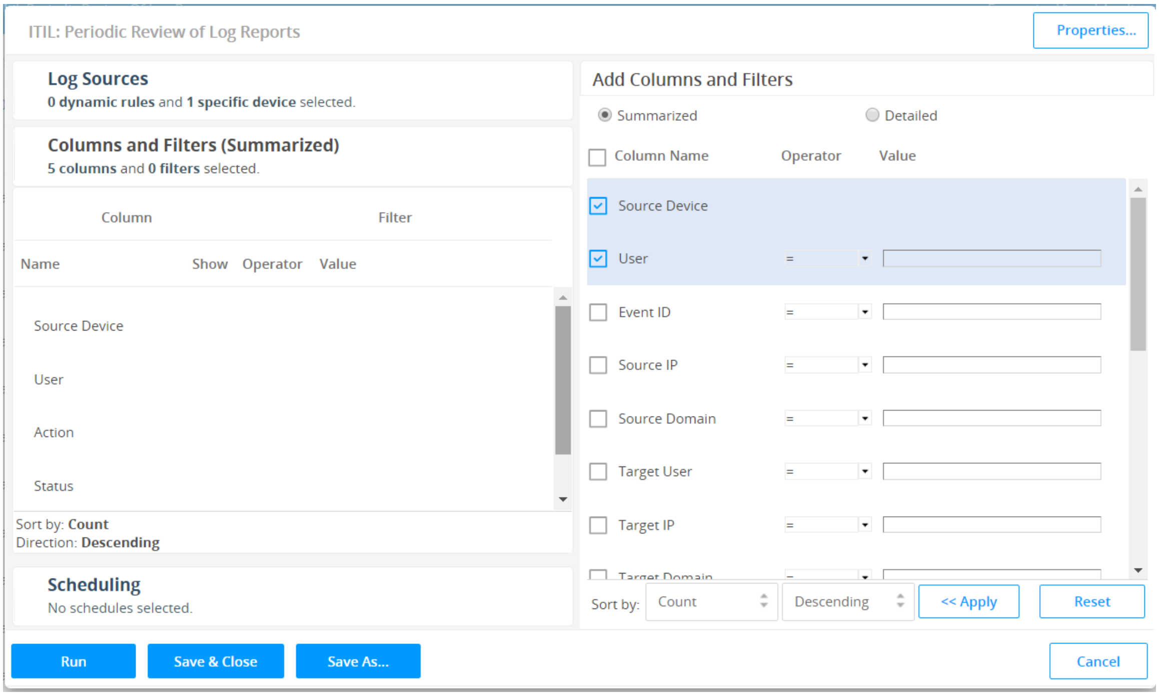
Procedure

1. Make sure that you are on the **Reports** page and click the **Edit** button of a report you want to modify.
2. Modify the report details (i.e., name, description, etc.), filters, and parameters.

   TIBCO LogLogic enables you to customize everything pertaining to the summarization and presentation of the reports. You can modify the device(s) on which the report runs, schedule when the report runs, and in the **Columns and Filters** area you can set specific report search filters.

   The following figure shows the report filters available under **Colmns and Filters** as well as the report details under **Update Saved Custom Report**.

   Advanced Options and Update Saved Custom Report Views



ITIL: Periodic Review of Log Reports

Log Sources
0 dynamic rules and 1 specific device selected.

Columns and Filters (Summarized)
5 columns and 0 filters selected.

Column		Filter	
Name	Show	Operator	Value
Source Device			
User			
Action			
Status			

Sort by: Count
Direction: Descending

Scheduling
No schedules selected.

Add Columns and Filters

● Summarized ○ Detailed

	Column Name	Operator	Value
☑	Source Device		
☑	User	=	
☐	Event ID	=	
☐	Source IP	=	
☐	Source Domain	=	
☐	Target User	=	
☐	Target IP	=	
☐	Target Domain	=	

Sort by: Count Descending

It is a good practice to test your modifications to ensure that the report meets your business needs.

3. To test the report, click **Run**.

   The report runs and returns data based on the set parameters. Verify that the returned data is what you want. Continue modifying and testing the report as needed.
4. Save the report by completing the following steps:

   a) Click **Save As**.

   Make any necessary modifications to the report details (i.e., **Report Name, Report Description**, etc.).

   b) Click **Save & Close**.

   A report saved message appears. Your report is now modified. Consider testing the output of the report again to ensure you are returning all of the data you need from this report.

The Compliance Suite Alerts

The TIBCO LogLogic® Compliance Suite - ITIL Edition alerts enable you to manage activities helping you to maintain ITIL and ITSM compliance. Activities can include detecting unusual traffic on your network or detecting Appliance system anomalies.

By default, the Compliance Suite alerts are disabled so that you can configure your environment with only those alerts that are necessary. For a description of all alerts in this Compliance Suite, see TIBCO LogLogic Alerts for ITIL

Accessing Available Compliance Suite Alerts

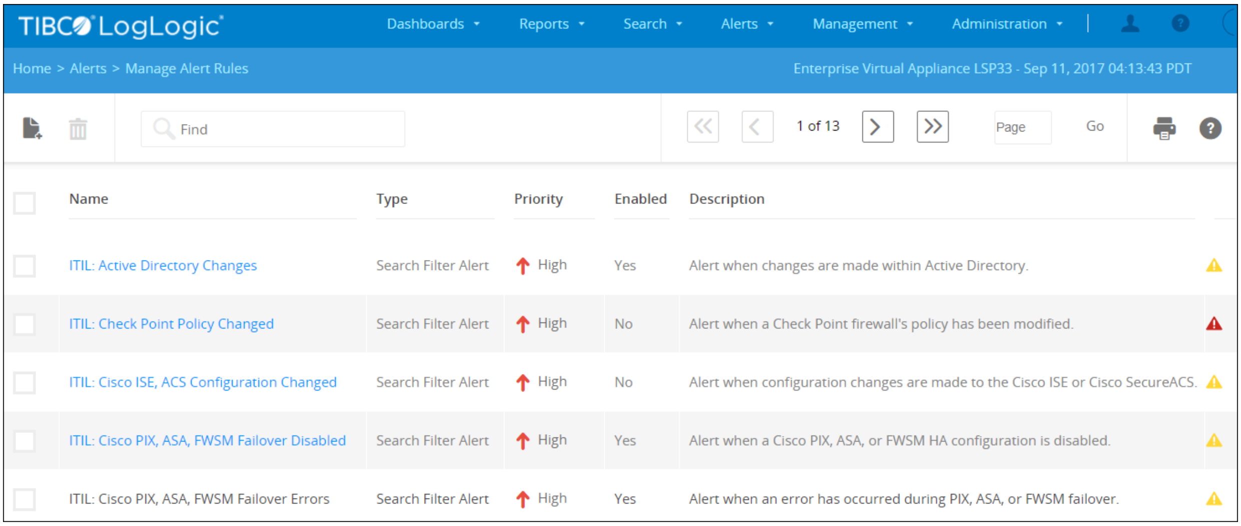
The Compliance Suite contains a number of alerts that can be easily enabled and modified for your business needs.

Procedure

1. From the navigation menu, click **Alerts** > **Manage Alert Rules** .

   The following figure shows a cropped list of the Compliance Suite alerts loaded from the ITIL XML file.

   Compliance Suite Alerts


TIBCO LogLogic
Dashboards
Reports
Search
Alerts
Management
Administration
Home > Alerts > Manage Alert Rules
Enterprise Virtual Appliance LSP33 - Sep 11, 2017 04:13:43 PDT
Find
1 of 13
Page
Go

□	Name	Type	Priority	Enabled	Description	
□	ITIL: Active Directory Changes	Search Filter Alert	↑ High	Yes	Alert when changes are made within Active Directory.	⚠
□	ITIL: Check Point Policy Changed	Search Filter Alert	↑ High	No	Alert when a Check Point firewall's policy has been modified.	⚠
□	ITIL: Cisco ISE, ACS Configuration Changed	Search Filter Alert	↑ High	No	Alert when configuration changes are made to the Cisco ISE or Cisco SecureACS.	⚠
□	ITIL: Cisco PIX, ASA, FWSM Failover Disabled	Search Filter Alert	↑ High	Yes	Alert when a Cisco PIX, ASA, or FWSM HA configuration is disabled.	⚠
□	ITIL: Cisco PIX, ASA, FWSM Failover Errors	Search Filter Alert	↑ High	Yes	Alert when an error has occurred during PIX, ASA, or FWSM failover.	⚠

2. To view details of a specific alert, click the **Name** of the alert.

   The **General** tab is selected by default, but each tab on the page contains information required to enable an alert.

3. Click on each of the tabs to view the default entries.

   Make sure that you identify the default entries and areas that might need to be modified.

Enabling Compliance Suite Alerts

By default, compliance suite alerts have pre-configured information to help you get started. In some instances, you can simply enable the alert because the default settings are aimed at capturing a broad range of alerts.

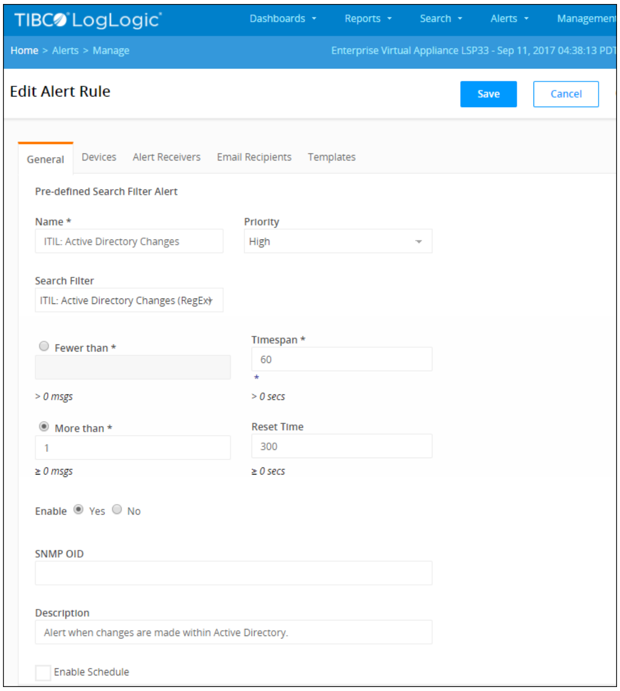
To enable alerts, you must set the device(s) to monitor, the SNMP trap receivers, as well as who receives an alert notification and how they receive it.

Procedure

1. From the navigation menu, select **Alerts** > **Manage Alert Rules** .
2. Click the **Name** of the alert.
3. On the **General** tab, for **Enable** select the **Yes** radio button.

   The following figure shows the **General** tab for the **ITIL: Active Directory Changes** alert.

   Active Directory Changes Alert



Edit Alert Rule

Pre-defined Search Filter Alert

Name * ITIL: Active Directory Changes

Priority High

Search Filter ITIL: Active Directory Changes (RegEx)

○ Fewer than *

> 0 msgs

Timespan * 60

> 0 secs

● More than * 1

≥ 0 msgs

Reset Time 300

≥ 0 secs

Enable ● Yes ○ No

SNMP OID

Description Alert when changes are made within Active Directory.

□ Enable Schedule

4. Select the device(s) to be alerted on by completing the following steps:

   You can define alerts for all devices, a selection of devices, or a single device.

   a) Select the **Devices** tab.

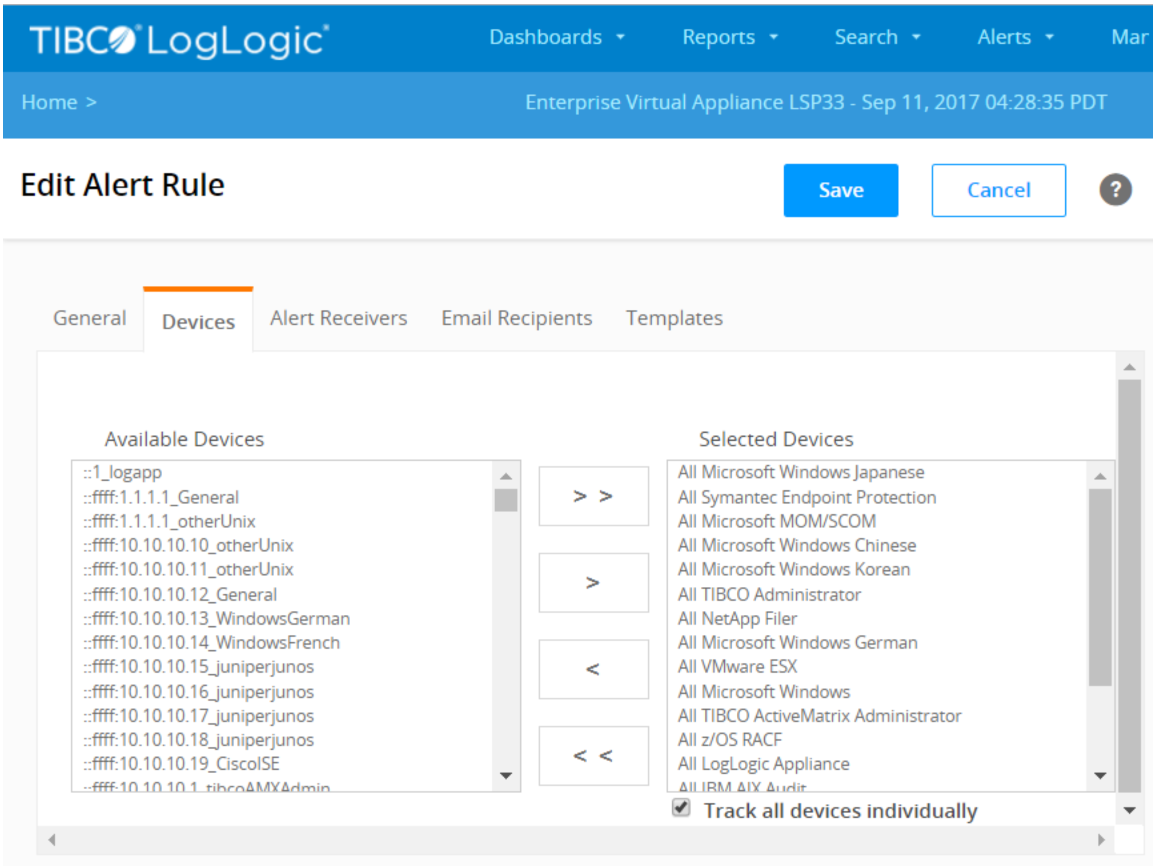
   b) In the **Available Devices** text block, select the appropriate log sources (that is devices) you want to monitor and be alerted on when an alert rule is triggered.

   > If the **Show Only Device Groups** setting is enabled on the Appliance, then the **Available Devices** text block lists only device groups. To enable or disable this feature, go to **Administration** > **System Settings** > **General** tab, scroll down to the **System** Performance Settings section and modify the **Optimize Device Selection List** option.

   c) Click **Add All** or **Add Selected Device(s)**.

   The following figure shows the **Devices** tab for the selected alert.

Available and Selected Devices



Available Devices

::1_logapp
::ffff:1.1.1.1_General
::ffff:1.1.1.1_otherUnix
::ffff:10.10.10.10_otherUnix
::ffff:10.10.10.11_otherUnix
::ffff:10.10.10.12_General
::ffff:10.10.10.13_WindowsGerman
::ffff:10.10.10.14_WindowsFrench
::ffff:10.10.10.15_juniperjunos
::ffff:10.10.10.16_juniperjunos
::ffff:10.10.10.17_juniperjunos
::ffff:10.10.10.18_juniperjunos
::ffff:10.10.10.19_CiscoISE
::ffff:10.10.10.1_tibcoAMXAdmin

Selected Devices

All Microsoft Windows Japanese
All Symantec Endpoint Protection
All Microsoft MOM/SCOM
All Microsoft Windows Chinese
All Microsoft Windows Korean
All TIBCO Administrator
All NetApp Filer
All Microsoft Windows German
All VMware ESX
All Microsoft Windows
All TIBCO ActiveMatrix Administrator
All z/OS RACF
All LogLogic Appliance
All IBM AIX Audit

☑ Track all devices individually

5. The Appliance has the ability to generate an SNMP trap that is sent to an SNMP trap receiver when an alert rule is triggered. Select the alert receivers available to your device(s) by completing the following steps:
   a) Select the **Alert Receivers** tab.
   b) In the **Available Alert Receivers** text block, select the appropriate alert receivers available for your device(s).
   c) Click **Add All** or **Add Selected Receiver(s)**.
6. Select the email recipients to be alerted with a notification email when an alert rule is triggered by completing the following steps:
   a) Select the **Email Recipients** tab.
   b) In the **Available Users** text block, select the appropriate email recipients.

      The **Available Users** text block lists all of the user accounts on the Appliance.
   c) Click **Add All** or **Add Selected User(s)**.
7. Click **Update**.

Viewing Compliance Suite Alert Results

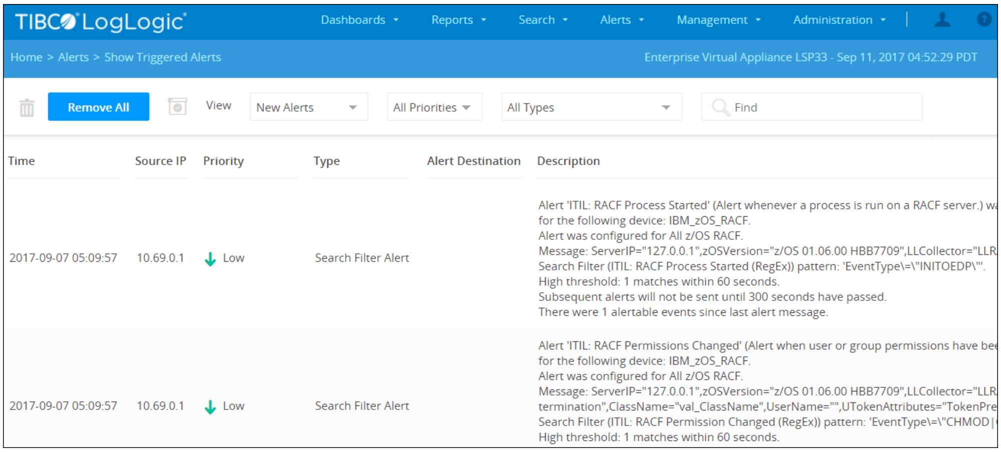
After you have enabled at least one alert, and that alert is triggered, you can view the results.

Procedure

1. In the navigation menu, select **Alerts** > **Show Triggered Alerts** .

   The following figure shows a cropped version of the **Show Triggered Alerts** page.

Aggregated Alert Log



Time	Source IP	Priority	Type	Alert Destination	Description
2017-09-07 05:09:57	10.69.0.1	↓ Low	Search Filter Alert		Alert 'ITIL: RACF Process Started' (Alert whenever a process is run on a RACF server.) wa for the following device: IBM_zOS_RACF. Alert was configured for All z/OS RACF. Message: ServerIP="127.0.0.1",zOSVersion="z/OS 01.06.00 HBB7709",LLCollector="LLR Search Filter (ITIL: RACF Process Started (RegEx)) pattern: 'EventType\=\"INITOEDP\"'. High threshold: 1 matches within 60 seconds. Subsequent alerts will not be sent until 300 seconds have passed. There were 1 alertable events since last alert message.
2017-09-07 05:09:57	10.69.0.1	↓ Low	Search Filter Alert		Alert 'ITIL: RACF Permissions Changed' (Alert when user or group permissions have bee for the following device: IBM_zOS_RACF. Alert was configured for All z/OS RACF. Message: ServerIP="127.0.0.1",zOSVersion="z/OS 01.06.00 HBB7709",LLCollector="LLR termination",ClassName="val_ClassName",UserName="",UTokenAttributes="TokenPre Search Filter (ITIL: RACF Permission Changed (RegEx)) pattern: 'EventType\=\"CHMOD| High threshold: 1 matches within 60 seconds.

2. From the **Show** drop-down menus, select the desired alert and priority filters to show only those alerts you want to display. The defaults are **New Alerts** and **All Priorities**.

3. (Management Station Appliances Only) From the **From Appliance** drop-down menu, select the Appliance from which you want to view the alerts.

4. View the results of your query. You can navigate through all of the data by using the page navigation buttons or page text field.

5. You can either acknowledge or remove an alert. Click the checkbox next to the alert name, then click either **Acknowledge, Remove**, or **Remove All**.

Each alert was triggered based on your set alert parameters, so care must be taken when acknowledging or removing the alert.

Service Delivery

Service Level Management

The goal for Service Level Management is to maintain and gradually improve IT Service quality, by defining, measuring and reporting upon a set of quality targets or Service Level Agreements (SLAs) between (internal or external) IT provider and IT customer. As such, Service Level Management for IT is not unlike Six Sigma continuous improvement for manufacturing.

Most companies today have implemented some SLAs to manage the relationship between IT provider and IT customer. The biggest problem is to find an effective way to measure and monitor pre-SLA achievements and to verify that targets are achievable before committing to them. Also, if SLAs are not focused and precise, then they may fall into disuse or even disrepute.

While Service Unavailability and Mean Time Between Failure are popular SLA measures, these measures alone are not sufficient to measure customer satisfaction. Other indicators such as throughput activity, traffic volume and transaction response times are needed as well.

A Key Performance Indicator (KPI) for Service Level Management is “coverage” or the percentage of services that are covered by SLAs. Commercial SLA monitoring tools exist, but most have a narrow and specific focus: one tool can monitor performance of web-based applications, while another focuses on e-mail or firewalls. Legacy and homegrown applications are notoriously difficult to integrate into commercial SLA tools and it is fair to say to that there is not a single product that can measure everything.

Log Intelligence can help to establish a baseline of pre-SLA performance and then use the same measures to identify post-SLA improvements. Simple and precise measurements can be derived for practically any service or system. All IT systems have some logs and, at a minimum, report on errors and reboots. Frequently, more granular records are available such a record for each successful or failed transaction, which a Log Intelligence solutions can use to compile statistics on the number of transactions processed.

Log Intelligence can provide a simple, accurate way to measure a variety of performance indicators that go beyond unavailability and Mean Time Between Failure, for all IT Services. Log data is natively available for all applications and do not require the installation of additional software on the application.

Service Level Management: Assess

As detailed in the Service Level Management ITSM process, before the IT organization can control and improve SLAs, IT organizations must first identify which IT services are being delivered and baseline the current performance level for each service. SLAs can be tied to an IT Service as a whole, such as the ‘e-mail service’ or to an IT System, such as “firewalls”.

Before negotiating SLAs all stakeholders should have a common, objective picture of current performance levels. No final SLA should be agreed upon or implemented before real monitoring data is collected to ensure that targets are achievable and an ongoing monitoring infrastructure is in place. The initial assessment of performance levels can also help to identify the weakest areas in the business, most in need of improvement, so a plan can be put in place to improve those areas first.

Log Intelligence can be used to assess the current performance of IT services and systems, such as by counting:

- # Error messages from firewalls, routers, switches, servers, and applications
- # Reboots for firewalls, routers, switches, servers, and applications
- # Transactions, e-mail messages, logins or connections processed (un)successfully
- Average (and minimum and maximum) transaction delay (such as mail delay)

The result of the assessment can also be correlated with data from assessment of the Incident Management or Capacity Management process. By comparing data across processes, management can establish whether:

- The number of Incidents reported to the support desk rise as SLA targets are being violated
- SLA targets are negatively impacted as capacity utilization targets are exceeded

Senior management can now use the result of the assessment to evaluate whether the correct assumptions have been made about the cause and effect of other processes on service quality.

Service Level Management: Monitor

Immediately once the SLA targets have been set, ongoing monitoring must start and periodic service achievement reports must be generated. The ITSM Service Level Management process recommends that operational reports must be generated at least daily and ideally real-time alerts should be triggered when SLAs are violated or threatened. In addition, periodic reports must be circulated to customers and IT managers with details of SLA performance and violations.

The service support desk should be notified immediately when SLAs are violated or threatened. Automated Log Intelligence can trigger alerts automatically based on preconfigured thresholds. A baseline of normal behavior can also be established automatically. Pro-active alerts can be generated when the number of log messages received is unusually high or low or when pre-determined ratios, such as unsuccessful/successful logins are unusual. An unusually low transaction (log message) rate can be a reliable early indicator that the service is degrading and may become unavailable in the near future. Such baseline alerts are particularly useful for legacy and homegrown applications, for which no other real-time SLA monitoring tools exist.

Service Level Management: Measure

In addition to real-time monitoring of SLA violations, service providers and customers should periodically review the achieved service levels and compare those to agreed upon targets. ITSM Service Level Management recommends that such meetings take place monthly or at least quarterly. The production of reports for these reviews can be extremely time-consuming and should be automated as much as possible. Log Intelligence solutions can automatically e-mail performance reports to customers and IT managers a couple of days ahead of the meeting.

At the meetings, particular attention should be paid to the root-cause of SLA violations and what can be done to prevent future instances. In some cases, it may become necessary to adjust SLA targets or to initiate a specific Service Improvement Program (SIP). In some cases SLA measures can also be used as a basis for charge-back relationships internally.

Service Level Management: Validate

In order to prove to customers and IT management that the Services Level Agreements have been met and targeted improvements are successful, IT organizations can use the collective record of periodic performance reviews. Performance data – including the raw data generated by the IT systems – can be archived as indisputable proof in case future disputes arise.

Service Level Management: Reports and Alerts

Use the following link/reference to see the Service Level Management reports and alerts:

Service Level Management.

Capacity Management

The Capacity Management process in ITSM is defined as the process that ensures the capacity of the IT infrastructure can meet the demands of the business in the most cost effective manner. The goal of Capacity Management is to prevent performance bottlenecks from impacting Service Availability or Performance pro-actively. This requires a process of comparing actual utilization with documented capacity thresholds in a near real-time fashion.

Utilization should be measured for all hardware (servers, mainframes, etc.), networking equipment (routers, VPN concentrators, firewalls, etc.), software (database applications, enterprise applications including homegrown systems) and human resources. By monitoring trends in resource utilization, utilization anomalies can be identified, which are early indicators of threatened Service Level misses.

Some organizations consider installing dedicated monitors on individual hardware and software components to monitor Resource utilization. This could be a hugely time consuming and expensive. External monitors can negatively impact resource performance and require expensive maintenance and upkeep. In addition, no monitor can report the whole picture. It is no surprise that in many organizations, the first time administrators engage in Capacity Management is when they receive complaints from users about Service performance. In other situations, a sample set of resources is monitored to approximate utilization. The bad news: all individual resources have finite capacity, which, when exceeded, will threaten service availability or performance.

The good news: nearly all IT resources already have built-in instrumentation in the form of log data. Logging just needs to be turned on. Log data, when combined with automated aggregation, alerting and reporting, provides a complete and cost-effective record of system activity and utilization. In fact, since the same Log Intelligence infrastructure is used for seven other ITSM processes, the incremental costs of Capacity Management are near-zero.

The activities as part of Capacity Management that can be supported by log data are:

- Planning for IT Resource Capacity to meet the needs of the business
- Monitoring of utilization of IT resources
- Tuning resources for optimal efficiency and performance

Capacity Management: Assess

Before a Capacity Plan can be put together, the organization needs to understand normal operating levels and the practical capacity of IT resources. Most manufacturers quoted performance numbers are not achievable in a production environment and thus need to be assessed empirically. Log data plays an important role in this assessment. By analyzing log data, a pattern or baseline of current usage can be established. By monitoring Service Levels and Incident Report rates in parallel, the actual resource capacity can be determined.

Log Intelligence reports that can be used to assess and baseline utilization:

- VPN utilization patterns
- Network traffic patterns
- Server, application, and information level access patterns
- E-mail traffic patterns

Capacity Management: Monitor

Rather than installing agent-based monitors, utilization can be very effectively monitored through log data especially considering that a Log Intelligence infrastructure is typically already in place to support other ITSM processes. Log data can be automatically analyzed against pre-set thresholds to trigger warnings. Many applications also have built-in thresholds and will automatically generate log messages when the application is nearing capacity. For example, most systems will warn when disk space, or CPU utilization are nearing capacity. No external instrumentation is required for this type of monitoring other than a log management system to receive and display (or transfer) the warning.

Typical capacity related alerts that can be triggered based on log data include when thresholds are exceeded for:

- CPU utilization
- Memory utilization
- Transactions (messages) per second
- Bandwidth utilization
- Total number of logins
- Total number of (VPN, Firewall) connections
- Frequency of data or program access

All thresholds should be set for the normal operating level as determined during the assessment phase. There should still be sufficient time to take corrective action before SLAs are breached.

In addition to static, manually configured thresholds, Log Intelligence solutions can also automatically create a baseline of normal activity levels. If these levels are exceeded an alarm can be triggered.

Capacity Management: Measure

When log data is stored over periods of times, it is possible to analyze daily, weekly, monthly and annual trends and to adjust Capacity Plans based on this analysis. Resources may be added or removed or rebalanced. Typically there are huge differences between average utilization and peak utilization and both should be recorded and taken into account.

Periodically, an effort should be undertaken to use utilization data to tune resources for optical performance. Using Log Intelligence reports you could for example:

- Tune firewall performance by analyzing firewall policy utilization: firewall performance will improve if frequently used rules are moved to the top whereas unused rules are removed from the system
- Tune file system performance by distributing frequently accessed files over different servers - or otherwise balance workload over various servers and applications
- Balancing the number of access requests by VPN concentrators can improve the connection speed for individual users

Capacity Management: Validate

In order to justify costly upgrades or expansion projects to senior management, it helps to have predictions available based on:

- Historical utilization trend data
- Proven correlation between under provisioning services and SLA impacts

In turn, IT Management can look at utilization reports to validate that capacity investments were made in the right areas at the right time: unnecessary spare capacity is as bad as too little capacity. By comparing actual utilization levels to predictions of the IT team or customer at the time of expansion, management can hold the team accountable for its actions.

Capacity Management: Reports and Alerts

Use the following link/reference to see the Capacity Management reports and alerts:

Capacity Management.

IT Service Continuity Management

IT Service Continuity Management (ITSCM) in ITSM is defined as the ability of a business to continue to satisfy pre-determined Service Level Agreements after a business interruption. A business interruption could be a system outage or the loss of an entire business site. ITSCM deals with major disasters and (prolonged) system failures with high cost of downtime. Routine failures are not considered business interruptions, but are addressed by Availability Management.

As businesses become more reliant on IT, continued availability of IT is critical to a company's survival. Increasingly, a large percentage of a company's market capitalization is linked to intellectual property that is stored digital format on IT systems. Therefore, a pro-active approach to IT Service Continuity Management, including IT asset and IT data protection, is now a fiduciary responsibility and Directors who do not take this task seriously are personally liable.

Defining the ITSCM strategy starts with conducting a thorough assessment of all the potential risks threatening continuity and by systematically designing ways to mitigate these risks. Risks that should be taken into account range from loss of physical IT systems and loss of network connectivity to loss of data. There are a wide range of systems and methods available to mitigate these risks: from redundant hardware configurations such as RAID arrays, mirrored or clustered systems, daily backups and a fully redundant disaster recovery data center. No matter what continuity solution is deployed, it is critical to monitor and validate that the Service Continuity infrastructure is functioning properly.

Log data can provide such assurance that the continuity infrastructure is in place and ready for action by monitoring error messages, activity levels and confirmation of successful procedures such as daily backups.

IT Service Continuity Management: Assess

ITSCM starts with the identification of the most critical and valuable IT Resources. Next, availability of these critical IT Resources should be monitored and reported on. Lastly, alternative processing as well as backup and recovery procedures should be designed for these most valuable and critical Resources.

Log data can help with each of these steps. First, log data can help with the assessment of risks to the business. Processed log data in the form of utilization data contains important clues about the value of IT Resources. The more business transactions are processed by a System, the more valuable it is to the business. Similarly, the more frequently programs and information are accessed, the higher the impact of discontinuity.

IT Service Continuity Management: Monitor

The most critical IT Resources should be monitored for availability as defined by the ITSM Availability Management process. Additional protection should be designed against major disasters and organizations should monitor vigorously that these protection mechanisms are enforced and working properly.

As a minimum, procedures should be in place to back up data and programs based on IT and user requirements. Organizations should define and implement procedures for backup and restoration of systems, data and documentation in line with business requirements and the continuity plan.

Log Intelligence solutions can monitor backup and restoration procedures and other ITSCM systems in real-time to validate its proper functioning. Log data reports and alerts are capable of extracting system records that validate when and if a backup was performed and if the backup is an exact copy of the original. TIBCO LogLogic can monitor systems to ensure that data backups are successfully accomplished on time and so that data restores are possible. They can also monitor and alert on when a data restore is completed successfully or unsuccessfully so that the integrity of backup data is retained in the event of a need to exercise a disaster recovery plan.

Log based warnings to monitor in real-time include:

- Disk failure errors

- Disk full notification messages
- Backup errors
- RAID errors

IT Service Continuity Management: Measure

Regular reports should be produced to measure the compliance with and effectiveness of ITSCM procedures. To ensure that ITSCM procedures are followed and that all ITSCM systems are operational, these reports should be reviewed regularly by customers and IT management. Reports of successful backups and log data of failover tests are one example of such validation.

IT Service Continuity Management: Validate

Senior management in its turn wants to use these reports as irrefutable proof to the board that they have fulfilled their fiduciary responsibility of verifying and testing the ITSCM infrastructure.

IT Service Continuity Management: Reports and Alerts

Use the following link/reference to see the IT Service Continuity Management reports and alerts:

Continuity Management.

Availability Management

As with IT Service Continuity Management, the importance of Availability Management has never been more apparent. Whereas ITSCM deals with major disasters, Availability Management deals with IT Service and component level outages. Availability is a key measure of most Service Level Agreements. Effective Availability Management is considered a primary factor influencing customer satisfaction and company reputation.

Note that for customers even performance degradation can be considered “Unavailability” of a Service. The goal of the ITSM Availability Management process is to cost-effectively meet an agreed upon level of required Availability and to continuously reduce the frequency and duration of Availability Incidents over time (without incurring extra costs).

It is important to recognize that when things go wrong, it is still possible to achieve business and user satisfaction. The way in which the organization handles Unavailability is just as important as the frequency and duration of outages. In addition to preventing Availability Incidents, companies should always look for ways to accelerate Service recovery and maintaining good communication with customers throughout the process.

The lifecycle of an Availability Incident can be divided into the following stages:

- Start
- Detect
- Diagnose
- Repair
- Recover
- Restore

Log Intelligence is not aiming to replace mature Availability and Systems Management solutions, but rather to enhance these in critical areas. Behavioral anomaly detection based on log information can enhance detection of incidents through mechanisms available in other Availability and System Management tools. Failure alerts can also be generated for legacy and homegrown systems that could otherwise not be monitored by these commercial tools.

Log data can also play an important role in accelerating the diagnosis and repair of Availability Incidents. Diagnosis is the process of determining the root-cause of a Service interruption. This stage tends to take up a considerable portion of the time to recovery and thus is a prime candidate for recovery acceleration. Diagnosis is also critical to analyze “what happened” after the fact and to ensure that steps are taken to prevent similar Availability Incidents in the future.

Log data can accelerate time to root-cause diagnosis and repair by providing investigative data at the fingertips of the analysts. In fact, most analysts turn to log data as a first step to figuring out “what happened”. It is critical to collect and retain 100% of log data because for diagnostic purposes. It is impossible to predict ahead of time what information is going to be necessary to diagnose and recover from an outage.

Availability Management: Assess

As with ITSCM, a record of Service and Component utilization constructed from log data can help identify the most critical assets to protect from Availability Incidents. There is strong correlation between Security Management and Availability Management as well. Even when IT Systems are technically available, data on the system can be Unavailable to a particular user if access rights are configured inappropriately. If Security is set too loosely, this results in Security, Privacy and Information Leakage risk for the organization. If Security is set too tightly, it will result in a higher Availability Incident rate because customers can’t access the data they need when they need it.

Therefore it is recommended that access to information is not restricted too tightly. It is better to err on the side of giving employees and customers access to information, while at the same time monitoring access to that information via log intelligence. Log monitoring provides a complete audit trail of user activity and acts as a powerful deterrent of misuse while maintaining Availability of Service.

Availability Management: Monitor

Availability and System Management tools focus on the detection, alerting, escalation and notification of IT failures. Log Intelligence can enhance the speed and accuracy of detection by enhancing System Management products with unique alert types. An automatic baseline can be established of the common message rate for a particular IT Component and any deviation against the baseline is reported to the Systems Management console:

- An unusually low message rate is a reliable indicator of performance degradation that could end in a Service or Component failure
- An unusual ratio between accepted and denied connections or successful and unsuccessful logins is an other indicator of a Service anomaly that requires immediate attention
- Search filter based alerts can be configured for legacy and homegrown applications that could otherwise not be integrated into the System Management

Only if the failure cause is known the System Management tools is able to perform auto-recovery actions. However, in most instances considerable “manual” diagnostic analysis is required to identify the root-cause of an Incident. Instant access to system activity log records can significant speed up the diagnosis:

- Access to the chronological sequence of actions and events performed by and on a Component during the ten minutes before failure to look for unusual events, such as a spike in utilization or a recent change in configuration that may have caused the failure
- Search for past events with a error code in the raw log data archives
- Search for similar events on other devices in the raw log data archives

After every incident a meeting should be convened to determine the root-cause of the Incident and to agree on steps to prevent similar Incidents in the future. The log data audit trail also fulfills an important role in this process.

Availability Management: Measure

Availability is measured by recording the frequency and duration of Availability Incidents as well as its scope impact. The ITSM process recommends that scope impact is measured by a combination of user minutes lost and business transactions lost. Transactions lost can easily be calculated if log data is at hand. The log data record will have recorded the number of business transactions per second at the time of the service interruption.

Log Intelligence can only be effective if a complete record of system activity and log data is available at all times. It is simply impossible to predict ahead of time which information is going to be needed so instead a complete “replay” of events should be available for search and reporting.

Availability Management: Validate

As with Service Level Management, log data can significantly enhance the coverage of executive Availability reporting. Log data is available for all Systems, including homegrown and legacy Systems. Therefore, log data is the lowest common denominator providing key Availability statistics for all Systems that can be collected, analyzed and archived over long periods of time and form the basis of Service Availability validation.

Availability Management: Reports and Alerts

Use the following link/reference to see the Availability Management reports and alerts:

Availability Management.

Service Support

Incident Management

ITSM defines incidents as events that are not part of the normal operation and have adverse impact on the business operations, such as network or system interruptions. When an incident occurs and causes reduction in the quality of services, the Incident Management process is specifically created to help restore the IT services back to its normal operations as quickly as possible so that the service is operating within the parameters of the service level agreement (SLA).

It's important to know that ITSM makes distinctions between an incident, a problem and a known error. An incident causes interruptions to normal operations. For example, an incident can be the server or network device going down, or an application bug preventing users from working was identified, or the printer not printing.

A problem occurs when the underlying cause for the incident or incidents cannot be identified. Sometimes several incidents may occur before a problem is recognized. The incidents in this case are symptoms of the problem. Often the incidents are resolved by simply fixing the symptoms. However, until the underlying cause is identified and fixed, a problem will eventually re-occur.

A problem record becomes a known error once it has been successfully diagnosed and a work-around has been developed. Log Intelligence can be used to detect any new incidents occurring in the IT infrastructure and alert IT organizations. In addition, Log Intelligence can be used to report on the number of instances that have occurred in the past to determine whether newly implemented ITSM processes are indeed effective.

Incident Management: Assess

As detailed in the Incident Management ITSM process, IT organizations should develop a knowledge base in the form of an up-to-date problem/error database. Although many IT organizations will develop this knowledge base after the Incident Management process has been implemented, Log Intelligence platforms can be used to pre-build this knowledge base before the actual implementation.

IT organizations can review all of the alerts that have been generated by Log Intelligence to:

- Understand previous Incidents in terms of failure rate, devices or device types that fail most often and when do most Incidents occur
- Identify existing Problems, e.g., incidents that occur repeatedly
- Compare these Problems to existing knowledge base to determine workarounds, thus building up a list of Known Errors

In addition, IT organizations can perform long-term searches or reports on the Log Intelligence platform to identify any Incidents that were not previously detected.

Incident Management: Monitor

Many organizations have implemented technologies such as network or system management platforms to help monitor the IT infrastructure. These platforms periodically poll the network devices and servers to determine whether they are still operational and available. The polling interval is usually configurable. Depending on the number of IT components being monitored, the interval can range from seconds to minutes.

However, because the polling interval can be minutes, many times when an IT component fails, it will take minutes for these management platforms to notice the failure. In addition, if the IT component fails temporary and restores service before the next poll, sometimes these management platforms may not even notice the failure.

Most of the network devices, servers and applications will generate log messages as they encounter errors. Log messages can indicate a network device is about to reboot due to errors, or a server has been restarted, or a routing failure has occurred. These log messages can act as warnings to the IT organization before disaster hits.

An effective Incident Management process requires real-time and automated incident detection mechanisms. Log Intelligence can be used as the foundation to continuously monitor the IT infrastructure and detect any faults or errors. Log Intelligence platforms can complement the existing management solutions by:

- Continuously monitor all logs generated by the IT infrastructure, also those from homegrown and legacy systems that are not otherwise tied into the System Management architecture
- Identify log messages that could act as a warning and alert administrators as needed
- Notify administrators when a device, server or application has failed
- Send alerts to Incident Management or Problem Management technologies to create tickets for tracking.
- Eliminate lost or incorrect Incidents by providing detailed information related to the incidents

In addition to alerting when an incident occurs, IT organizations can also utilize Log Intelligence to obtain details of the incident in order to investigate and diagnose the incident. Also, administrators can collect and analyze all relevant log information related to the incident. Real-time monitoring ensures the impact to the business is minimized, e.g., reduce the number of people or systems affected.

Incident Management: Measure

Accurate monitoring of the Incident Management process allows performance against SLAs to be accurately measured. Key Performance Indicators (KPI) of the Incident Management process recommends that the metrics to be defined early on in the implementation process in order to judge process performance and have measurable targets. These metrics can include:

- Number of incidents detected during a specific period of time
- Number of incidents resolved
- Amount of time took to resolve the incidents
- Number of problems resulted from the detected incidents

Log Intelligence can be used to periodically generate reports that can assist Incident Managers to measure the performance of the Incident Management process. For example, by comparing the weekly reports from Log Intelligence, Incident Managers can quickly determine the trend of the incident count.

Utilizing the same reports as described in the Assess step, Incident Managers can also determine whether multiple Incidents are symptoms of a Problem. Identified Problems can then quickly be escalated to the Problem Management process for verification and resolution.

Incident Management: Validate

In order to prove to senior management that the process improvements are successful, IT organizations must validate that the goals established are met at the end of the project.

Incident Management: Reports and Alerts

Use the following link/reference to see the Incident Management reports and alerts:

Incident Management.

Problem Management

A problem occurs when the underlying cause for the incident or incidents cannot be identified. Sometimes several incidents may occur before a problem is recognized. The incidents in this case are symptoms of the problem. Often the incidents are resolved by simply fixing the symptoms. However, until the underlying cause is identified and fixed, a problem will eventually re-occur.

The ITSM Problem Management process is designed to detect underlying causes, identify workarounds and provide resolutions to Incidents. A successful implementation of the Problem Management process should help IT organizations minimize the adverse impact of Incidents and Problems to the business. The goal of the Incident Management process is to restore services as quickly as possible. The goal of the Problem Management process is to determine permanent resolutions.

The problem management system should provide for adequate audit trail facilities that allow tracking, analyzing, and determining the root cause of all reported problems considering:

- All associated configuration items
- Outstanding problems and incidents
- Known and suspected errors

Managing problems and incidents addresses how an organization identifies documents and responds to events that fall outside of normal operations. IT organizations must maintain a complete and accurate audit trail for network devices, servers and applications, This enables IT to address how business identify root causes of issues that may introduce inaccuracy in reporting. Also, the problem management system must provide for adequate audit trail facilities that allow tracing from incident to underlying cause.

Problem Management: Assess

As with Incident Management, IT organizations can use Log Intelligence to identify existing Problems in the IT infrastructure and build a knowledge base before the implementation of the Problem Management process.

The ITSM Problem Management process specifically recommends that IT organizations obtain statistics from current support activities as a basis. Understanding the existing state of the IT infrastructure allows the IT organization to define specific goals that can be measured. Furthermore, IT organizations should set achievable objectives in advance.

IT organizations can use Log Intelligence solutions to:

- Obtain statistics of Incidents happened previously in the IT infrastructure
- Determine patterns of failures, including which IT components fail most often, which location, whether or not they were user errors, machine errors or process errors

Problem Management: Monitor

As explained in the Problem Management process, Problems and Known Errors can be identified by analyzing Incidents as they occur and/or over a differing time period. Log Intelligence solutions can be used to alert on any failures as they occur. Administrators can then respond rapidly to potential problems and incidents that might affect availability, security, or performance. Real-time data monitoring and reporting capabilities reduce time to repair after incidents, reducing costs, and improving application availability.

Given that the goal of Problem Management is to determine the underlying root cause of the Incidents, IT organizations can utilize the vast amount of log information gathered on the Log Intelligence solutions to perform investigations. IT organizations can:

- Use alerts to actively monitor any reoccurrence of the same Incidents. This may allow IT administrators to identify patterns that were not previously seen.

- Use log searches and reports to identify events that happened before and after the Incidents.

Problem Management: Measure

Quality of service and performance of the Problem Management process can be measured using detailed historical information. Periodic audits can also confirm that the Problem Management teams are following the predefined procedures. Problem Management teams and their customers should agree on a reporting schedule early on in the implementation process.

Log Intelligence solutions can be used to:

- Provide detailed reports on a list of Incidents occurred in the IT infrastructure. This list of Incidents can be compared to the related Problems to ensure Problems have been correctly diagnosed and resolved.
- Identify further Incidents that occur after the Problem has been resolved. These Incidents may indicate that the Problem has not been fully diagnosed.

Problem Management: Validate

In order to prove to senior management that the process improvements are successful, IT organizations must validate that the goals established are met at the end of the project.

Problem Management: Reports and Alerts

Use the following link/reference to see the Problem Management reports and alerts:

Problem Management.

Configuration Management

Configuration management is the control of changes made to all hardware and software configurations. ITSM describes these as configuration items (CI) and can include configuration settings and policies, user accounts and access permissions. Most IT organizations recognize the need to implement a comprehensive Configuration Management Database (CMDB) to assist their quest in improving service quality. However, even though CMDB technologies are getting more wide spread, not all IT infrastructure has been incorporated into the CMDB, especially older applications, mainframe applications, or even brand new applications that CMDB technologies do not have built-in models.

To complement the CMDB implementations, IT organizations should implement additional technologies, such as TIBCO LogLogic® Log Management Intelligence (LMI), to provide a comprehensive view of all hardware, software and application configuration changes. In addition, many IT organizations recognize that over-bureaucratic change management processes will increase the time it takes to make configuration changes and diminish process effectiveness. To increase efficiency and decrease configuration time, IT organizations are starting to adjust their processes to allow approved standard changes to take place without going through formal change management processes.

However, with this new process, some of the changes will no longer be documented by the change management system. It is crucial that IT organization periodically review all configuration changes to ensure they are appropriate and authorized. Log Intelligence solution can be used to report on all configuration changes, including hardware, software and applications that are not managed by the CMDB technologies. Log Intelligence can also report on all configuration changes so the IT organizations can review and adjust the process as needed.

Configuration Management: Assess

As detailed in the Configuration Management ITSM process, before the IT organization can control configuration management and only allow authorized and approved changes, IT organizations must identify the configuration structure and understand their current state.

Log Intelligence solution can be used to assess several aspect of the current configuration state, including:

- Assess the frequency of changes being made to critical IT infrastructures such as network devices and applications
- Identify the users and IP addresses that are making these critical changes
- Determine changes that are made often as they might be candidates for standard changes
- Establish configuration change trends such as days of the week when most changes occur
- Verify that all changes made are in fact the same as the CMDB record

The result of the assessment can also be correlated with data from assessment of the Incident Management process. For example, the correlated result may indicate that:

- More incidents are reported when many configuration changes occur in a short period of time
- More incidents are reported when a certain user is making these changes
- More incidents are reported when a particular web proxy configuration was made

Senior management can now use the result of the assessment to set goals and directions on what improvements must be made to the Configuration Management process.

Configuration Management: Monitor

Most IT organizations have accepted that CMDB is a critical component in implementing the ITSM processes. To ensure a successful outcome of the implementation, IT organizations should establish processes in the beginning of the project to perform continuous monitoring of all configuration changes.

Log Intelligence can be used to alert on all configuration changes by any network devices, systems or applications. Whenever a change is made to a configuration item, the IT administrators are immediately notified. The IT administrators can then compare this alerted change to the CMDB being implemented to ensure it has been appropriately approved.

Continuous monitoring using TIBCO LogLogic provides several benefits to the implementation of the CMDB. First, by alerting changes made in real-time allow IT administrators to quickly identify holes in the implementation process and ensure that all critical IT components are covered. Second, continuously monitoring allows standard change candidates be identified early on. The IT administrators can then adjust the implementation process to incorporate the standard changes. Third, even after the implementation of the CMDB, some users can still circumvent the established processes to make unauthorized changes. By continuously monitoring all configuration changes, the IT organization can ensure all changes are made through the appropriate channels. Fourth, continuous monitoring through Log Management allows the IT organization to monitor changes to network devices, system and applications that are not part of the CMDB. Essentially, Log Intelligence is a great complement to the CMDB.

Configuration Management: Measure

What cannot be measured cannot be improved. Periodic measurement of the implementation results ensures that IT organizations know the effect of the implementation. Regular reporting of the measurements can identify adverse impacts the new process has on the IT organization as well as the business.

Using the same log information as the assessment stage, IT organizations should periodically compare the new measurement against assessment results. By doing so, IT organizations can:

- Understand how the new process or CMDB is improving Configuration Management process. Are there fewer incidents occurring during configuration changes?
- Confirm that the improvements are on track to meet the goals established in the beginning of the project.
- Identify, document, and institutionalize those tasks that are well known and approve them as standard changes.

- Determine whether existing standard changes are still appropriate as the organization changes.

Configuration Management: Validate

In order to prove to senior management that the process improvements are successful, IT organizations must validate that the goals established are met at the end of the project.

Configuration Management: Reports and Alerts

Use the following link/reference to see the Configuration Management reports and alerts:

Configuration Management.

Change Management

The goal of change management is to standardize the methods and procedures in which IT organizations use to modify hardware, communication equipment, software, systems and other “live” application software. This precludes applications under development. The Change Management process should be implemented in parallel with the Configuration Management processes. The Change Management process is responsible for assessing impacts on business and IT performance, and authorizing changes based on the impact assessment. On the other hand, Configuration Management is responsible for identifying all areas that will be impacted based on the Change Request, providing that information to Change Management so it can assess the impact, and finally update the configuration items with the requested changes.

Managing changes addresses how an organization modifies functionality to help the business meet its service level agreements. Deficiencies in this area may significantly impact the service level promised to the business. For example, changes to the programs that allocate data to accounts require appropriate approvals and testing prior to the change to ensure classification and data integrity.

Change management ensures that security, availability, and processing integrity controls are set up in the system and maintained through its life cycle. Insufficient configuration controls can lead to security and availability exposures that may permit unauthorized access to systems and data and impact reporting.

Change Management: Assess

Assessing the current state of Change Management process provides IT organizations a basis to start. By understanding the number of changes that were created because of identified Problems, which in turn were a set of Incidents, IT organizations can establish a baseline of the number of Incidents that became Problems that became Changes.

With this understanding, IT organizations can also measure the impact of the current Change Management process. Impact to the organization can include service quality, service availability, security, and customer satisfaction.

Log Intelligence can be used to:

- Identify all configuration changes performed on critical IT infrastructures
- Determine the number of Incidents and Problems resulted from the configuration changes
- Understand the trend of change requests such when do most changes occur and when do changes cause failures

Change Management: Monitor

Activity logs provide numerous ways to monitor system change activity to determine if change management procedures are correctly implemented and being followed. Change Managers can setup alerts to be notified when changes have been performed. This allows Change Managers to determine that changes indicated in the documentation have actually been implemented in the manner and at the time prescribed.

In addition, Change Managers can use these alerts to determine whether critical hardware and software changes were performed had gone through the Change Management process for approval.

Monitoring the changes made to critical IT infrastructure allows the IT organization to anticipate and detect problems that arise due to the changes. Businesses must also ensure that requests for program changes, system changes, and maintenance (including changes to system software) are standardized, documented, and subject to formal change management procedures.

IT organizations should:

- Have reports that identify all changes to network devices, systems and applications and ensure that all changes are authorized. The most efficient way to identify configuration changes is at the time of the modification. Administrators should setup alerts so that any changes to the configuration, authorized or otherwise, are detected and notified.
- Have reports that monitor all changes to the production environment and compare the changes to documented approvals utilizing alerts and reports on policy modifications, groups activities, escalated privilege activities, permissions changed.
- Validate that application software and data storage systems are properly configured to provision access based on the individual’s demonstrated need to view, add, change or delete data.

Change Management: Measure

Periodic reports of the Changes made to the IT infrastructure should be provided to the Change Managers and the senior management so they can observe the progress of the Change Management implementation.

It’s likely different management level will require different levels of information. For example, CIOs may require a quarterly high-level overview of the number of changes made vs. the number of unauthorized changes made. Service managers may require detailed weekly reports listing the individual changes made and the status of the change. Log Intelligence reports can be produced to:

- Identify changes made to network device and system configurations
- Determine whether a large number of changes have been made to a configuration item
- Confirm all changes made are either standard changes or have been approved by the Change Advisory Board (CAB)

Furthermore, results from these reports can be correlated with reports from Incident Management or Problem Management to:

- Understand how the Change Requests affect the number of incidents or problems
- Confirm that by following formal change management processes, service quality has indeed improved (e.g., less failures or less back-outs)
- Determine whether the number of incidents have decreased, leading to fewer problems and additional change requests
- Demonstrate that implementing change management process has reduced disruption over time

Change Management: Validate

It is also recommended that Service Management review the change Management process periodically for efficiency and effectiveness. Such a review should be carried out shortly after the Change Management process is implemented, to ensure that the plans were carried out shortly after the Change Management process is implemented, to ensure that the plans were carried out correctly and that the process is functioning as intended.

Thereafter, regular formal reviews of the Change Management process should take place – at least every six months. To satisfy this control objective, administrators must review all changes to the production environment and compare the changes to documented approvals to ensure the approval process is followed. From the archived audit log data, obtain a sample of regular and emergency changes made to applications/systems to determine whether they were adequately tested and approved before being placed into a production environment. Trace the sample of changes back to the change request log and supporting documentation.

Change Management: Reports and Alerts

Use the following link/reference to see the Change Management reports and alerts:

Change Management.

TIBCO LogLogic Reports and Alerts for ITIL

- TIBCO LogLogic Reports for ITIL
- TIBCO LogLogic Alerts for ITIL
- TIBCO LogLogic Reports and Alerts Quick Reference

TIBCO LogLogic Reports for ITIL

The following table lists the reports included in theTIBCO LogLogic® Compliance Suite - ITIL Edition.

Serial Number	TIBCO LogLogic Report	Description
1	ITIL: Active Directory System Changes	Displays changes made within Active Directory.
2	ITIL: Check Point Configuration Changes	Displays all Check Point audit events related to configuration changes.
3	ITIL: Cisco ESA: Attacks by Event ID	Displays Cisco ESA attacks by Event ID.
4	ITIL: Cisco ESA: Attacks Detected	Displays attacks Detected by Cisco ESA.
5	ITIL: Cisco ESA: Attacks by Threat Name	Displays Cisco ESA attacks by threat name.
6	ITIL: Cisco ESA: Scans	Displays scans using Cisco ESA.
7	ITIL: Cisco ESA: Updated	Displays updates to Cisco ESA.
8	ITIL: Cisco ISE, ACS Configuration Changes	Displays Cisco ISE and Cisco SecureACS configuration changes.
9	ITIL: Cisco PIX, ASA, FWSM Fa ilover Disabled	Displays all logs related to disabling Cisco PIX, ASA, and FWSM failover capability.
10	ITIL: Cisco PIX, ASA, FWSM Fa ilover Errors	Displays events indicating the PIX, ASA, and FWSM devices have failover errors.
11	ITIL: Cisco PIX, ASA, FWSM Fa ilover Performed	Displays all logs related to performing a Cisco PIX, ASA, and FWSM failover.
12	ITIL: Cisco PIX, ASA, FWSM P olicy Changed	Displays all configuration changes made to the Cisco PIX, ASA, and FWSM devices.
13	ITIL: Cisco PIX, ASA, FWSM R estarted	Displays all Cisco PIX, ASA, or FWSM restart activities to detect unusual activities.

Serial Number	TIBCO LogLogic Report	Description
14	ITIL: Cisco PIX, ASA, FWSM Routing Failure	Displays all Cisco PIX, ASA, and FWSM routing error messages.
15	ITIL: Cisco Routers and Switches Restart	Displays all Cisco routers and switches restart activities to detect unusual activities.
16	ITIL: Cisco Switch Interface Down	Displays events indicating the Cisco Switches' interface has gone down.
17	ITIL: Cisco Switch Interface Up	Displays events indicating the Cisco Switches' interface has gone up.
18	ITIL: Cisco Switch Policy Changes	Displays all configuration changes to the Cisco router and switch policies.
19	ITIL: DHCP Granted/Renewed Activities on Microsoft DHCP	Displays all DHCP Granted/Renewed activities on Microsoft DHCP Server.
20	ITIL: DHCP Granted/Renewed Activities on VMware vShield	Displays all DHCP Granted/Renewed activities on VMware vShield Edge.
21	ITIL: DNS Server Error	Displays all events when DNS Server has errors.
22	ITIL: Domain activities on Symantec Endpoint Protection	Displays all domain activities on Symantec Endpoint Protection.
23	ITIL: Domains Sending the Most Email - Exchange 2000/2003	Displays the top domains sending email.
24	ITIL: Email Domains Experiencing Delay - Exchange 2000/2003	Displays the recipient domains that have experienced the most delivery delays.
25	ITIL: Email Recipients Receiving the Most Emails by Count - Exchange 2007/10	Displays the email recipients who receiving the most emails by count.
26	ITIL: Email Senders Sending the Most Emails by Count - Exchange 2007/10	Displays the email senders who sent the most emails by count.
27	ITIL: Email Source IP Sending to Most Recipients	Displays IP addresses that are sending to the most recipients using Exchange 2007/10.
28	ITIL: ESX Kernel log daemon terminating	Displays all VMware ESX Kernel log daemon terminating.
29	ITIL: ESX Kernel logging Stop	Displays all VMware ESX Kernel logging stops.
30	ITIL: ESX Syslogd Restart	Displays all VMware ESX syslogd restarts.

Serial Number	TIBCO LogLogic Report	Description
31	ITIL: F5 BIG-IP TMOS Restarted	Displays all events when the F5 BIG-IP TMOS has been restarted.
32	ITIL: Firewall Traffic by Rule - Check Point	Displays all network traffic flowing through each rule in a network policy to ensure appropriate access.
33	ITIL: FireEye MPS: Attacks by Event ID	Displays FireEye MPS attacks by Event ID.
34	ITIL: FireEye MPS: Attacks by Threat Name	Displays FireEye MPS attacks by threat name.
35	ITIL: FireEye MPS: Attacks Detected	Displays attacks detected by FireEye MPS.
36	ITIL: Firewall Traffic by Rule - Juniper Firewall	Displays all network traffic flowing through each rule in a network policy to ensure appropriate access.
37	ITIL: Firewall Traffic by Rule - Nortel	Displays all network traffic flowing through each rule in a network policy to ensure appropriate access.
38	ITIL: FortiOS: Attacks by Event ID	Displays FortiOS attacks by Event ID.
39	ITIL: FortiOS: Attacks by Threat Name	Displays FortiOS attacks by threat name.
40	ITIL: FortiOS: Attacks Detected	Displays attacks detected by FortiOS.
41	ITIL: FortiOS DLP Attacks Detected	Displays all DLP attacks detected by FortiOS.
42	ITIL: HP NonStop Audit Configuration Changes	Displays all audit configuration changes on HP NonStop.
43	ITIL: HP NonStop Audit Login Failed	Displays all HP NonStop Audit login events which have failed.
44	ITIL: HP NonStop Audit Object Changes	Displays HP NonStop Audit events related to object changes.
45	ITIL: HP NonStop Audit Permissions Changed	Displays all permission modification activities on HP NonStop Audit to ensure authorized access.
46	ITIL: i5/OS Backup Configuration Changes	Lists all events when the i5/OS backup options have been modified.
47	ITIL: i5/OS Object Permissions Modified	Displays all permission modification activities on i5/OS to ensure authorized access.
48	ITIL: i5/OS Restarted	Lists all events when the i5/OS has been restarted.

Serial Number	TIBCO LogLogic Report	Description
49	ITIL: i5/OS Service Started	Lists all events when a user starts a service on the i5/OS.
50	ITIL: Juniper Firewall Restarted	Displays all Juniper Firewall restart events.
51	ITIL: Juniper Firewall HA State Changed	Displays all Juniper firewall fail-over state change events.
52	ITIL: Juniper Firewall Policy Ch anged	Displays all configuration changes to the Juniper Firewall policies.
53	ITIL: Juniper Firewall Policy O ut of Sync	Displays events that indicate the Juniper Firewall's HA policies are out of sync.
54	ITIL: Juniper Firewall Reset Acc epted	Displays events that indicate the Juniper Firewall has been reset to its factory default state.
55	ITIL: Juniper Firewall Reset Imminent	Displays events that indicate the Juniper Firewall will be reset to its factory default state.
56	ITIL: LogLogic Disk Full	Displays events that indicate the LogLogic appliance's disk is near full.
57	ITIL: LogLogic HA State Chang ed	Displays all LogLogic appliance failover state change events.
58	ITIL: LogLogic Management Center Backup Activities	Displays all backup activities on LogLogic management center.
59	ITIL: LogLogic Management Center Restore Activities	Displays all restore activities on LogLogic management center.
60	ITIL: LogLogic Management Center Upgrade Success	Displays all successful events related to the system's upgrade.
61	ITIL: LogLogic Universal Collector Configuration Changes	Displays LogLogic universal collector configuration changes.
62	ITIL: Microsoft Operations Manager - Windows Permissions Modified	Displays all permission modification activities on Windows servers to ensure authorized access.
63	ITIL: Microsoft Operations Manager - Windows Policies Modified	Displays all policy modification activities on Windows servers to ensure authorized and appropriate access.
64	ITIL: Microsoft Operations Manager - Windows Servers Restarted	Displays all Windows server restart activities to detect unusual activities.

Serial Number	TIBCO LogLogic Report	Description
65	ITIL: Microsoft Sharepoint Permissions Changed	Displays all user/group permission events to Microsoft Sharepoint.
66	ITIL: Microsoft Sharepoint Policy Add, Remove, or Modify	Displays all events when a Microsoft Sharepoint policy is added, removed, or modified.
67	ITIL: Most Active Ports Through Firewall - Check Point	Displays the most active ports used through the Check Point firewall.
68	ITIL: Most Active Ports Through Firewall - Cisco ASA	Displays the most active ports used through the Cisco ASA firewall.
69	ITIL: Most Active Ports Through Firewall - Cisco FWSM	Displays the most active ports used through the Cisco FWSM firewall.
70	ITIL: Most Active Ports Through Firewall - Cisco Netflow	Displays the most active ports used through the Cisco Netflow.
71	ITIL: Most Active Ports Through Firewall - Cisco PIX	Displays the most active ports used through the Cisco PIX firewall.
72	ITIL: Most Active Ports Through Firewall - Fortinet	Displays the most active ports used through the Fortinet firewall.
73	ITIL: Most Active Ports Through Firewall - Juniper Firewall	Displays the most active ports used through the Juniper firewall.
74	ITIL: Most Active Ports Through Firewall - Nortel	Displays the most active ports used through the Nortel firewall.
75	ITIL: Most Active Ports Through Firewall - PANOS	Displays the most active ports used through the PANOS firewall.
76	ITIL: McAfee AntiVirus: Attacks by Event ID	Displays McAfee AntiVirus attacks by Event ID.
77	ITIL: McAfee AntiVirus: Attacks by Threat Name	Displays McAfee AntiVirus attacks by threat name.
78	ITIL: McAfee AntiVirus: Attacks Detected	Displays attacks detected by McAfee AntiVirus.
79	ITIL: NetApp Filer Audit Login Failed	Displays all NetApp Filer Audit Login events which have failed.
80	ITIL: NetApp Filer Audit Policies Modified	Displays all policy modification activities on NetApp Filer Audit to ensure authorized and appropriate access.

Serial Number	TIBCO LogLogic Report	Description
81	ITIL: NetApp Filer Boot Block Updated	Displays all events indicating that the boot block has been updated on the NetApp Filer.
82	ITIL: NetApp Filer Disk Failure	Displays all disk failure events on the NetApp Filer servers.
83	ITIL: NetApp Filer Login Failed	Displays all NetApp Filer Login events which have failed.
84	ITIL: NetApp Filer Disk Missing	Displays events that indicate disk missing on the NetApp Filer servers.
85	ITIL: NetApp Filer File System Full	Displays events that indicate the NetApp Filer's disk is near full.
86	ITIL: NetApp Filer RAID Disk Inserted	Displays all events related to disk insertion into the NetApp Filer RAID.
87	ITIL: NetApp Filer RAID Disk Pulled	Displays all events related to disk removal into the NetApp Filer RAID.
88	ITIL: NetApp Filer Snapshot Error	Displays events that indicate backup on the NetApp Filer has failed.
89	ITIL: NTP Daemon Exited	Displays events that indicate the NTP service has stopped.
90	ITIL: NTP Server Unreachable	Displays events that indicate the remote NTP server is not reachable.
91	ITIL: PANOS: Attacks by Event ID	Displays Palo Alto Networks attacks by Event ID.
92	ITIL: PANOS: Attacks by Threat Name	Displays Palo Alto Networks attacks by threat name.
93	ITIL: PANOS: Attacks Detected	Displays attacks detected by Palo Alto Networks.
94	ITIL: Periodic Review of Log Reports	Displays all review activities performed by administrators to ensure review for any access violations.
95	ITIL: Permissions Modified on Windows Servers	Displays all permission modification activities on Windows servers to ensure authorized access.
96	ITIL: Policies Modified on Windows Servers	Displays all policy modification activities on Windows servers to ensure authorized and appropriate access.
97	ITIL: RACF Permissions Changed	Displays all permission modification activities on RACF to ensure authorized access.

Serial Number	TIBCO LogLogic Report	Description
98	ITIL: RACF Process Started	Displays all processes started on the RACF servers.
99	ITIL: Software Update Successes on i5/OS	Displays all i5/OS successful events related to the system's software or patch update.
100	ITIL: Symantec AntiVirus: Attacks by Threat Name	Displays Symantec AntiVirus attacks by threat name.
101	ITIL: Symantec AntiVirus: Attacks Detected	Displays attacks detected by Symantec AntiVirus.
102	ITIL: Symantec AntiVirus: Scans	Displays scans using Symantec AntiVirus.
103	ITIL: Symantec AntiVirus: Updated	Displays updates to Symantec AntiVirus.
104	ITIL: Symantec Endpoint Protection: Attacks by Threat Name	Displays Symantec Endpoint Protection attacks by threat name.
105	ITIL: Symantec Endpoint Protection: Attacks Detected	Displays attacks detected by Symantec Endpoint Protection.
106	ITIL: Symantec Endpoint Protection Configuration Changes	Displays Symantec Endpoint Protection configuration changes.
107	ITIL: Symantec Endpoint Protection Policy Add, Remove, or Modify	Displays all events when a Symantec Endpoint Protection policy is added, removed, or modified.
108	ITIL: Symantec Endpoint Protection: Scans	Displays scans using Symantec Endpoint Protection.
109	ITIL: Symantec Endpoint Protection: Updated	Displays updates to Symantec Endpoint Protection.
110	ITIL: System Restarted	Displays all logs related to system restarts.
111	ITIL: TIBCO Administrator Login Failed	Displays all TIBCO Administrator Login events which have failed.
112	ITIL: TIBCO ActiveMatrix Administrator Failed Logins	Displays all TIBCO ActiveMatrix Administrator Login events which have failed.
113	ITIL: TIBCO Administrator Permission Changes	Displays events related to TIBCO Administrator permission modifications.

Serial Number	TIBCO LogLogic Report	Description
114	ITIL: TIBCO ActiveMatrix Administrator Permission Changes	Displays events related to TIBCO ActiveMatrix Administrator permission modifications.
115	ITIL: TrendMicro OfficeScan: Attacks Detected	Displays attacks detected by TrendMicro OfficeScan.
116	ITIL: TrendMicro OfficeScan: Attacks Detected by Threat Name	Displays attacks detected by TrendMicro OfficeScan by threat name.
117	ITIL: TrendMicro Control Manager: Attacks Detected	Displays attacks detected by TrendMicro Control Manager.
118	ITIL: TrendMicro Control Manager: Attacks Detected by Threat Name	Displays attacks detected by TrendMicro Control Manager by threat name.
119	ITIL: UNIX Failed Logins	Displays failed UNIX logins for known and unknown users.
120	ITIL: vCenter Change Attributes	Modification of VMware vCenter and VMware ESX properties.
121	ITIL: vCenter Modify Firewall Policy	Displays changes to the VMware ESX allowed services firewall policy.
122	ITIL: vCenter Orchestrator Change Attributes	Modification of VMware vCenter Orchestrator properties.
123	ITIL: vCenter Orchestrator Virtual Machine Created	Virtual machine has been created from VMware vCenter Orchestrator.
124	ITIL: vCenter Orchestrator Virtual Machine Deleted	Virtual machine has been deleted from VMware vCenter Orchestrator.
125	ITIL: vCenter Orchestrator Virtual Machine Shutdown	Virtual machine has been shutdown or paused from VMware vCenter Orchestrator console.
126	ITIL: vCenter Orchestrator Virtual Machine Started	Virtual machine has been started or resumed from VMware vCenter Orchestrator console.
127	ITIL: vCenter Orchestrator vSwitch Added, Changed or Removed	vSwitch has been added, modified or removed from VMware vCenter Orchestrator console.
128	ITIL: vCenter Resource Usage Change	Resources have changed on VMware vCenter.
129	ITIL: vCenter Restart ESX Services	VMware vCenter restarted services running on VMware ESX Server.

Serial Number	TIBCO LogLogic Report	Description
130	ITIL: vCenter Shutdown or Restart of ESX Server	VMware ESX Server is shutdown or restarted from VMware vCenter console.
131	ITIL: vCenter User Permission Change	A permission role has been added, changed, removed, or applied to a user on VMware vCenter server.
132	ITIL: vCenter Virtual Machine Created	Virtual machine has been created from VMware vCenter console.
133	ITIL: vCenter Virtual Machine Deleted	Virtual machine has been deleted or removed from VMware vCenter console.
134	ITIL: vCenter Virtual Machine Shutdown	Virtual machine has been shutdown or paused from VMware vCenter console.
135	ITIL: vCenter Virtual Machine Started	Virtual machine has been started or resumed from VMware vCenter console.
136	ITIL: vCenter vSwitch Added, Changed or Removed	vSwitch on VMware ESX server has been added, modified or removed from the VMware vCenter console.
137	ITIL: vCloud Organization Created	VMware vCloud Director organization created events.
138	ITIL: vCloud Organization Deleted	VMware vCloud Director organization deleted events.
139	ITIL: vCloud Organization Modified	VMware vCloud Director organization modified events.
140	ITIL: vCloud vApp Created, Modified, or Deleted	VMware vCloud Director vApp created, deleted, and modified events.
141	ITIL: vCloud vDC Created, Modified, or Deleted	VMware vCloud Director virtual datacenter created, modified, or deleted events.
142	ITIL: VPN Connection Average Bandwidth	Displays the average bandwidth for VPN connections.
143	ITIL: VPN Connection Average Duration	Displays the average duration of VPN connections.
144	ITIL: vShield Edge Configuration Changes	Displays changes to VMware vShield Edge policies.
145	ITIL: Web URLs Visited	Displays URLs that have been visited.
146	ITIL: Web URLs Visited - F5 BIG-IP TMOS	Displays URLs that have been visited on F5 BIG-IP TMOS.

Serial Number	TIBCO LogLogic Report	Description
147	ITIL: Web URLs Visited - Fortinet	Displays URLs that have been visited on Fortinet.
148	ITIL: Web URLs Visited - Microsoft IIS	Displays URLs that have been visited on Microsoft IIS.
149	ITIL: Web URLs Visited - PANOS	Displays URLs that have been visited on Palo Alto Networks.
150	ITIL: Web URLs Visited via Proxy	Displays URLs that have been visited via a proxy server.
151	ITIL: Web URLs Visited via Proxy - Blue Coat Proxy	Displays URLs that have been visited via a proxy server on Blue Coat Proxy.
152	ITIL: Web URLs Visited via Proxy - Cisco WSA	Displays URLs that have been visited via a proxy server on Cisco WSA.
153	ITIL: Web URLs Visited via Proxy - Microsoft IIS	Displays URLs that have been visited via a proxy server on Microsoft IIS.
154	ITIL: Windows AD Backup Err or	Displays events indicating that Windows AD backup has errors.
155	ITIL: Windows AD Backup Fail ed	Displays events indicating that Windows AD backup has failed.
156	ITIL: Windows AD Backup Star ting	Displays events indicating that Windows AD backup has started.
157	ITIL: Windows AD Exception E rrors	Displays exception errors from Windows Active Directory.
158	ITIL: Windows AD Replication Error	Displays replication errors for Windows Active Directory.
159	ITIL: Windows AD Restore Fail ed	Displays events indicating restore of the Windows AD database has failed.
160	ITIL: Windows AD Startup	Displays events related to the start up of Windows Active Directory.
161	ITIL: Windows AD Unable to R ecover	Displays events indicating Windows AD has errored and cannot recover.
162	ITIL: Windows Domain Activities	Displays all trusted domains created or deleted on Windows servers to ensure authorized and appropriate access.
163	ITIL: Windows New Services In stalled	Displays a list of new services installed on Windows servers to ensure authorized access.

Serial Number	TIBCO LogLogic Report	Description
164	ITIL: Windows Servers Restarte d	Displays all Windows server restart activities to detect unusual activities.
165	ITIL: Windows Software Updat e Failures	Displays all failed events related to the system's software or patch update.
166	ITIL: Windows Software Updat e Successes	Displays all successful events related to the system's software or patch update.

TIBCO LogLogic Alerts for ITIL

The following table lists the alerts included in the TIBCO LogLogic® Compliance Suite - ITIL Edition.

Serial Number	TIBCO LogLogic Alert	Description
1	ITIL: Active Directory Changes	Alerts when changes are made within Active Directory.
2	ITIL: Check Point Policy Changed	Alerts when a Check Point firewall’s policy has been modified.
3	ITIL: Cisco ISE, ACS Configuration Changed	Alerts when configuration changes are made to the Cisco ISE or Cisco SecureACS.
4	ITIL: Cisco PIX, ASA, FWSM Failover Disabled	Alerts when a Cisco PIX, ASA, or FWSM HA configuration is disabled.
5	ITIL: Cisco PIX, ASA, FWSM Failover Errors	Alerts when an error has occurred during PIX, ASA, or FWSM failover.
6	ITIL: Cisco PIX, ASA, FWSM Failove r Performed	Alerts when a failover has occurred on the Cisco PIX, ASA, or FWSM devices.
7	ITIL: Cisco PIX, ASA, FWSM Policy Changed	Alerts when a Cisco PIX, ASA, or FWSM firewall policy has been modified.
8	ITIL: System Restarted	Alerts when system has been restarted.
9	ITIL: Cisco PIX, ASA, FWSM Routin g Failure	Alerts when routing failure occurred in the Cisco PIX, ASA, or FWSM devices.
10	ITIL: Cisco PIX, ASA, FWSM Shun Added	Alerts when a shun rule has been added to the PIX, ASA, or FWSM configuration.
11	ITIL: Cisco PIX, ASA, FWSM Shun Deleted	Alerts when a shun rule has been removed from the PIX, ASA, or FWSM configuration.

Serial Number	TIBCO LogLogic Alert	Description
12	ITIL: Cisco Routers and Switches Restarted	Alerts when Cisco routers or switches have been restarted.
13	ITIL: Cisco Switch Interface Down	Alerts when Cisco switch interface is going down.
14	ITIL: Cisco Switch Interface Up	Alerts when the Cisco switch interface is back up.
15	ITIL: Cisco Switch Policy Changed	Alerts when Cisco router or switch configuration has been modified.
16	ITIL: DNS Server Shutdown	Alerts when DNS Server has been shutdown.
17	ITIL: DNS Server Started	Alerts when DNS Server has been started.
18	ITIL: HP NonStop Audit Configuration Changed	Alerts when configuration changes are made to the HP NonStop Audit.
19	ITIL: HP NonStop Audit Permission Changed	Alerts on HP NonStop Audit permission changed events.
20	ITIL: i5/OS Server or Service Status Change	Alerts when the i5/OS is restarted or a service stops or starts.
21	ITIL: Juniper Firewall HA State Change	Alerts when Juniper Firewall has changed its failover state.
22	ITIL: Juniper Firewall Policy Changes	Alerts when Juniper Firewall configuration is changed.
23	ITIL: Juniper Firewall Policy Out of Sync	Alerts when the Juniper Firewall's policy is out of sync.
24	ITIL: Juniper Firewall Reset Imminent	Alerts when the Juniper Firewall will be reset to factory default.
25	ITIL: Juniper Firewall System Reset	Alerts when the Juniper Firewall has been reset to system default.
26	ITIL: Juniper VPN Policy Change	Alerts when Juniper VPN policy or configuration change.
27	ITIL: Juniper VPN System Error	Alerts when events related to the Juniper VPN system errors or failures are detected.
28	ITIL: LogLogic Disk Full	Alerts when the LogLogic appliance's disk is near full.

Serial Number	TIBCO LogLogic Alert	Description
29	ITIL: LogLogic HA State Change	Alerts when the LogLogic appliance failover state changes.
30	ITIL: LogLogic Management Center Backed Up or Restored	Alerts on backup and restore events to the LogLogic management center.
31	ITIL: LogLogic Management Center Upgrade Succeeded	Alerts for successful events related to the system's upgrade.
32	ITIL: LogLogic Universal Collector Configuration Changed	Alerts when configuration changes are made to the LogLogic universal collector.
33	ITIL: Microsoft Operations Manager - Permissions Changed	Alerts when user or group permissions have been changed.
34	ITIL: Microsoft Operations Manager - Windows Policies Changed	Alerts when Windows policies changed.
35	ITIL: Microsoft Operations Manager - Windows Server Restarted	Alerts when Windows server is restarted
36	ITIL: Microsoft Sharepoint Permission Changed	Alerts on Microsoft Sharepoint permission changed events.
37	ITIL: Microsoft Sharepoint Policies Added, Removed, Modified	Alerts on Microsoft Sharepoint policy additions, deletions, and modifications.
38	ITIL: NetApp Bootblock Update	Alerts when the bootblock has been updated on a NetApp Filer.
39	ITIL: NetApp Filer Audit Policies Changed	Alerts when NetApp Filer Audit policies changed.
40	ITIL: NetApp Filer Backup Errors	Alerts when the NetApp Filer has errors in the backups.
41	ITIL: NetApp Filer Disk Failure	Alerts when a disk fails on a NetApp FIler.
42	ITIL: NetApp Filer Disk Inserted	Alerts when a disk is inserted into the NetApp Filer.
43	ITIL: NetApp Filer Disk Missing	Alerts when a disk is missing on the NetApp Filer device.
44	ITIL: NetApp Filer Disk Pulled	Alerts when a RAID disk has been pulled from the Filer device.

Serial Number	TIBCO LogLogic Alert	Description
45	ITIL: NetApp Filer File System Full	Alerts when the file system is full on the NetApp Filer device.
46	ITIL: NetApp Filer Snapshot Error	Alerts when an error has been detected during a NetApp Filer snapshot.
47	ITIL: NTP Daemon Exited	Alerts when the NTP service has stopped.
48	ITIL: NTP Server Unreachable	Alerts when the remote NTP server is unreachable.
49	ITIL: Pulse Connect Secure Policy Change	Alerts when Pulse Connect Secure policy or configuration change.
50	ITIL: Pulse Connect Secure System Error	Alerts when events related to the Pulse Connect Secure system errors or failures are detected.
51	ITIL: RACF Permissions Changed	Alerts when user or group permissions have been changed.
52	ITIL: RACF Process Started	Alerts whenever a process is run on a RACF server.
53	ITIL: Symantec Endpoint Protection Configuration Changed	Alerts when configuration changes are made to the Symantec Endpoint Protection.
54	ITIL: Symantec Endpoint Protection Domains Created	Alerts when a new domain has been created on Symantec Endpoint Protection.
55	ITIL: Symantec Endpoint Protection Policy Add, Delete, Modify	Alerts on Symantec Endpoint Protection additions, deletions, and modifications.
56	ITIL: System Restarted	Alerts when systems such as routers and switches have restarted.
57	ITIL: TIBCO ActiveMatrix Administrator Permission Changed	Alerts on TIBCO ActiveMatrix Administrator permission changed events.
58	ITIL: vCenter Create Virtual Machine	Alerts when virtual machine has been created from VMware vCenter console.
59	ITIL: vCenter Delete Virtual Machine	Alerts when a virtual machine has been deleted or removed from VMware vCenter console.
60	ITIL: vCenter Firewall Policy Change	Alerts when changes to the VMware ESX allowed services firewall policy.
61	ITIL: vCenter Orchestrator Create Virtual Machine	Virtual machine has been created from VMware vCenter Orchestrator console.

Serial Number	TIBCO LogLogic Alert	Description
62	ITIL: vCenter Orchestrator Delete Virtual Machine	Alerts when a virtual machine has been deleted or removed from VMware vCenter Orchestrator console.
63	ITIL: vCenter Orchestrator Virtual Machine Shutdown	Virtual machine has been shutdown or paused from VMware vCenter Orchestrator console.
64	ITIL: vCenter Orchestrator Virtual Machine Started	Virtual machine has been started or resumed from VMware vCenter Orchestrator console.
65	ITIL: vCenter Orchestrator vSwitch Add, Modify or Delete	vSwitch on VMware ESX Server has been added, modified or removed from vCenter Orchestrator.
66	ITIL: vCenter Permission Change	Alerts when a permission role has been added, changed, removed, or applied on VMware vCenter.
67	ITIL: vCenter Restart ESX Services	Alerts when VMware vCenter restarted services running on VMware ESX Server.
68	ITIL: vCenter Shutdown or Restart ESX	Alerts when VMware ESX Server is shutdown from vCenter console.
69	ITIL: vCenter Virtual Machine Shutdown	Alerts when virtual machine has been shutdown or paused from VMware vCenter console.
70	ITIL: vCenter Virtual Machine Started	Alerts when virtual machine has been started or resumed from VMware vCenter console.
71	ITIL: vCenter vSwitch Add, Modify or Delete	Alerts when vSwitch on VMware ESX server has been added, modified or removed from vCenter.
72	ITIL: vCloud Organization Created	Alerts when organization successfully created on VMware vCloud Director.
73	ITIL: vCloud Organization Deleted	Alerts when organization successfully deleted on VMware vCloud Director.
74	ITIL: vCloud Organization Modified	Alerts when organization successfully modified on VMware vCloud Director.
75	ITIL: vCloud User, Group, or Role Modified	Alerts when VMware vCloud Director user, group, or role has been modified.
76	ITIL: vCloud vApp Created, Deleted, or Modified	Alerts when VMware vCloud Director vApp has been created, deleted, or modified.
77	ITIL: vCloud vDC Created, Modified, or Deleted	Alerts when VMware vCloud Director Virtual Datacenters have been created, deleted, or modified.
78	ITIL: VPN Connection Capacity Exceeded	Alerts when the VPN connection is exceeding estimated capacity.

Serial Number	TIBCO LogLogic Alert	Description
79	ITIL: vShield Edge Configuration Change	Alerts when configuration changes to VMware vShield Edge policies.
80	ITIL: Windows AD Backup Error	Alerts when backup has encountered errors for Windows AD.
81	ITIL: Windows AD Backup Failed	Alerts when backup has failed for Windows AD.
82	ITIL: Windows AD Backup Starting	Alerts when back is starting for Windows AD.
83	ITIL: Windows AD Replication Error	Alerts when replication has errors for Windows AD.
84	ITIL: Windows AD Restore Failed	Alerts when Windows AD database restoration has errors.
85	ITIL: Windows AD Startup	Alerts when Windows AD has been started.
86	ITIL: Windows Domains Created	Alerts when a new domain has been created for Windows.
87	ITIL: Windows New Services Installed	Alerts when a new service has been installed on Windows servers.
88	ITIL: Windows Permissions Changed	Alerts when user or group permissions have been changed.
89	ITIL: Windows Policies Changed	Alerts when Windows policies changed.
90	ITIL: System Restarted	Alerts when system has been restarted.
91	ITIL: Windows Software Updates	Alerts when events related to the Windows' software updates.

TIBCO LogLogic Reports and Alerts Quick Reference

The following table lists the reports and alerts included in the TIBCO LogLogic® Compliance Suite - ITIL Edition.

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
Service Delivery		

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
Service Level Management	LogLogic® LMI solution, in conjunction with the TIBCO LogLogic® Compliance Suite - ITIL Edition, provides the reports and alerts around which a variety of daily security operational procedures can be built or improved.	**Compliance Suite Reports** ITIL: Cisco PIX, ASA, FWSM Failover Errors ITIL: Cisco PIX, ASA, FWSM Failover Performed ITIL: Cisco PIX, ASA, FWSM Restarted ITIL: Cisco PIX, ASA, FWSM Routing Failure ITIL: Cisco Routers and Switches Restart ITIL: Cisco Switch Interface Down ITIL: Cisco Switch Interface Up ITIL: DHCP Granted/Renewed Activities on Microsoft DHCP ITIL: DHCP Granted/Renewed Activities on VMware vShield ITIL: DNS Server Error ITIL: Domains Sending the Most Email - Exchange 2000/2003 ITIL: Email Domains Experiencing Delay - Exchange 2000/2003 ITIL: Email Recipients Receiving the Most Emails by Count - Exchange 2007/10 ITIL: Email Senders Sending the Most Emails by Count - Exchange 2007/10 ITIL: Email Source IP Sending To Most Recipients ITIL: F5 BIG-IP TMOS Restarted ITIL: Firewall Traffic by Rule - Check Point ITIL: Firewall Traffic by Rule - Juniper Firewall ITIL: Firewall Traffic by Rule - Nortel ITIL: FireEye MPS: Attacks by Event ID ITIL: FireEye MPS: Attacks by Threat Name ITIL: FireEye MPS: Attacks Detected ITIL: HP NonStop Audit Login Failed ITIL: i5/OS Restarted ITIL: Juniper Firewall HA State Changed ITIL: Juniper Firewall Policy Changed

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
Service Level Management	LogLogic LMI solution, in conjunction with the TIBCO LogLogic® Compliance Suite - ITIL Edition, provides the reports and alerts around which a variety of daily security operational procedures can be built or improved.	**Compliance Suite Reports** (Cont.) ITIL: Juniper Firewall Policy Out of Sync ITIL: Juniper Firewall Reset Accepted ITIL: Juniper Firewall Restarted ITIL: Juniper Firewall Reset Imminent ITIL: LogLogic Disk Full ITIL: LogLogic HA State Changed ITIL: LogLogic Management Center Backup Activities ITIL: LogLogic Management Center Restore Activities ITIL: Microsoft Operations Manager - Windows Servers Restarted ITIL: Most Active Ports Through Firewall - Check Point ITIL: Most Active Ports Through Firewall - Cisco ASA ITIL: Most Active Ports Through Firewall - Cisco FWSM ITIL: Most Active Ports Through Firewall - Cisco Netflow ITIL: Most Active Ports Through Firewall - Cisco PIX ITIL: Most Active Ports Through Firewall - Fortinet ITIL: Most Active Ports Through Firewall - Juniper Firewall ITIL: Most Active Ports Through Firewall - Nortel ITIL: Most Active Ports Through Firewall - PANOS ITIL: NetApp Filer Audit Login Failed ITIL: NetApp Filer Disk Failure ITIL: NetApp Filer Disk Missing ITIL: NetApp Filer File System Full ITIL: NetApp Filer Login Failed ITIL: NetApp Filer RAID Disk Inserted ITIL: NetApp Filer RAID Disk Pulled ITIL: NetApp Filer Snapshot Error ITIL: NTP Daemon Exited ITIL: NTP Server Unreachable

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
Service Level Management	LogLogic LMI solution, in conjunction with the TIBCO LogLogic® Compliance Suite - ITIL Edition, provides the reports and alerts around which a variety of daily security operational procedures can be built or improved.	**Compliance Suite Reports** (Cont.) ITIL: Periodic Review of Log Reports ITIL: System Restarted ITIL: TIBCO Administrator Login Failed ITIL: TIBCO ActiveMatrix Administrator Failed Logins ITIL: UNIX Failed Logins ITIL: vCenter Orchestrator Virtual Machine Shutdown ITIL: vCenter Orchestrator Virtual Machine Started ITIL: vCenter Shutdown or Restart of ESX Server ITIL: vCenter Virtual Machine Shutdown ITIL: vCenter Virtual Machine Started ITIL: VPN Connection Average Bandwidth ITIL: VPN Connection Average Duration ITIL: Web URLs Visited via Proxy - Cisco WSA ITIL: Web URLs Visited - F5 BIG-IP TMOS ITIL: Web URLs Visited - Fortinet ITIL: Web URLs Visited - Microsoft IIS ITIL: Web URLs Visited - PANOSITIL: Web URLs Visited via Proxy ITIL: Web URLs Visited via Proxy - Blue Coat Proxy ITIL: Web URLs Visited via Proxy - Microsoft IIS ITIL: Windows AD Backup Error ITIL: Windows AD Backup Failed ITIL: Web URLs Visited ITIL: Windows AD Exception Errors ITIL: Windows AD Replication Error ITIL: Windows AD Restore Failed ITIL: Windows AD Startup ITIL: Windows AD Unable to Recover ITIL: Windows Servers Restarted ITIL: Windows Software Update Failures **Compliance Suite Alerts** ITIL: Cisco PIX, ASA, FWSM Failover Errors ITIL: Cisco PIX, ASA, FWSM Failover Performed

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
		ITIL: System Restarted
Service Level Management	LogLogic LMI solution, in conjunction with the TIBCO LogLogic® Compliance Suite - ITIL Edition, provides the reports and alerts around which a variety of daily security operational procedures can be built or improved.	**Compliance Suite Alerts** (Cont.) ITIL: Cisco PIX, ASA, FWSM Routing Failure ITIL: Cisco Routers and Switches Restarted ITIL: Cisco Switch Interface Down ITIL: Cisco Switch Interface Up ITIL: DNS Server Shutdown ITIL: DNS Server Started ITIL: Juniper Firewall HA State Change ITIL: Juniper Firewall Policy Out of Sync ITIL: Juniper Firewall Reset Imminent ITIL: Juniper Firewall System Reset ITIL: Juniper VPN System Error ITIL: LogLogic Disk Full ITIL: LogLogic HA State Change ITIL: LogLogic Management Center Backed Up or Restored ITIL: Microsoft Operations Manager - Windows Server Restarted ITIL: NetApp Filer Backup Errors ITIL: NetApp Filer Disk Failure ITIL: NetApp Filer Disk Missing ITIL: NetApp Filer Disk Pulled ITIL: NetApp Filer File System Full ITIL: NetApp Filer Snapshot Error ITIL: NTP Daemon Exited ITIL: Pulse Connect Secure System Error ITIL: System Restarted ITIL: vCenter Orchestrator Virtual Machine Shutdown ITIL: vCenter Orchestrator Virtual Machine Started ITIL: vCenter Shutdown or Restart ESX ITIL: vCenter Virtual Machine Shutdown ITIL: vCenter Virtual Machine Started ITIL: VPN Connection Capacity Exceeded

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
Service Level Management	LogLogic LMI solution, in conjunction with the TIBCO LogLogic® Compliance Suite - ITIL Edition, provides the reports and alerts around which a variety of daily security operational procedures can be built or improved.	**Compliance Suite Alerts** (Cont.) ITIL: Windows AD Backup Error ITIL: Windows AD Backup Failed ITIL: Windows AD Replication Error ITIL: Windows AD Restore Failed ITIL: Windows AD Startup ITIL: System Restarted
Capacity Management	LogLogic LMI solution, in conjunction with the TIBCO LogLogic® Compliance Suite - ITIL Edition, provides the reports and alerts around which a variety of daily security operational procedures can be built or improved.	**Compliance Suite Reports** ITIL: DHCP Granted/Renewed Activities on Microsoft DHCP ITIL: DHCP Granted/Renewed Activities on VMware vShield ITIL: Domains Sending the Most Email - Exchange 2000/2003 ITIL: Email Recipients Receiving the Most Emails by Count - Exchange 2007/10 ITIL: Email Senders Sending the Most Emails by Count - Exchange 2007/10 ITIL: Email Source IP Sending To Most Recipients ITIL: Firewall Traffic by Rule - Check Point ITIL: Firewall Traffic by Rule - Juniper Firewall ITIL: Firewall Traffic by Rule - Nortel ITIL: LogLogic Disk Full ITIL: NetApp Filer File System Full ITIL: Periodic Review of Log Reports ITIL: VPN Connection Average Bandwidth ITIL: VPN Connection Average Duration **Compliance Suite Alerts** ITIL: LogLogic Disk Full ITIL: NetApp Filer File System Full ITIL: VPN Connection Capacity Exceeded

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
Continuity Management	LogLogic LMI solution, in conjunction with the TIBCO LogLogic® Compliance Suite - ITIL Edition, provides the reports and alerts around which a variety of daily security operational procedures can be built or improved.	**Compliance Suite Reports** ITIL: Cisco PIX, ASA, FWSM Failover Disabled ITIL: Cisco PIX, ASA, FWSM Failover Errors ITIL: Cisco PIX, ASA, FWSM Failover Performed ITIL: DNS Server Error ITIL: Juniper Firewall HA State Changed ITIL: LogLogic Disk Full ITIL: LogLogic HA State Changed ITIL: LogLogic Management Center Backup Activities ITIL: LogLogic Management Center Restore Activities ITIL: NetApp Filer Disk Failure ITIL: NetApp Filer Disk Missing ITIL: NetApp Filer File System Full ITIL: NetApp Filer RAID Disk Inserted ITIL: NetApp Filer RAID Disk Pulled ITIL: NetApp Filer Snapshot Error ITIL: Periodic Review of Log Reports ITIL: Pulse Connect Secure Policy Change ITIL: Pulse Connect Secure System Error ITIL: Windows AD Backup Error ITIL: Windows AD Backup Failed ITIL: Windows AD Replication Error ITIL: Windows AD Restore Failed ITIL: Windows AD Unable to Recover **Compliance Suite Alerts** ITIL: Cisco PIX, ASA, FWSM Failover Disabled ITIL: Cisco PIX, ASA, FWSM Failover Errors ITIL: Cisco PIX, ASA, FWSM Failover Performed ITIL: Juniper Firewall HA State Change ITIL: LogLogic Disk Full ITIL: LogLogic HA State Change ITIL: LogLogic Management Center Backed Up or Restored ITIL: NetApp Filer Backup Errors

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
		ITIL: NetApp Filer Disk Failure ITIL: NetApp Filer Disk Inserted ITIL: NetApp Filer Disk Missing
Continuity Management	LogLogic LMI solution, in conjunction with the TIBCO LogLogic® Compliance Suite - ITIL Edition, provides the reports and alerts around which a variety of daily security operational procedures can be built or improved.	**Compliance Suite Alerts** (Cont.) ITIL: NetApp Filer Disk Pulled ITIL: NetApp Filer File System Full ITIL: NetApp Filer Snapshot Error ITIL: Pulse Connect Secure Policy Change ITIL: Pulse Connect Secure System Error ITIL: Windows AD Backup Error ITIL: Windows AD Backup Failed ITIL: Windows AD Replication Error ITIL: Windows AD Restore Failed

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
Availability Management	LogLogic LMI solution, in conjunction with the TIBCO LogLogic® Compliance Suite - ITIL Edition, provides the reports and alerts around which a variety of daily security operational procedures can be built or improved.	**Compliance Suite Reports** ITIL: Cisco ESA: Attacks by Event ID ITIL: Cisco ESA: Attacks Detected ITIL: Cisco ESA: Attacks by Threat Name ITIL: Cisco ESA: Scans ITIL: Cisco ESA: Updated ITIL: Cisco PIX, ASA, FWSM Failover Disabled ITIL: Cisco PIX, ASA, FWSM Failover Errors ITIL: Cisco PIX, ASA, FWSM Failover Performed ITIL: Cisco Switch Interface Down ITIL: Cisco Switch Interface Up ITIL: DHCP Granted/Renewed Activities on Microsoft DHCP ITIL: DHCP Granted/Renewed Activities on VMware vShield ITIL: DNS Server Error ITIL: FortiOS: Attacks by Event ID ITIL: FortiOS: Attacks by Threat Name ITIL: FortiOS: Attacks Detected ITIL: FortiOS DLP Attacks Detected ITIL: i5/OS Backup Configuration Changes ITIL: Juniper Firewall HA State Changed ITIL: LogLogic Disk Full ITIL: LogLogic HA State Changed ITIL: LogLogic Management Center Backup Activities ITIL: LogLogic Management Center Restore Activities ITIL: McAfee AntiVirus: Attacks by Event ID ITIL: McAfee AntiVirus: Attacks by Threat Name ITIL: McAfee AntiVirus: Attacks Detected ITIL: NetApp Filer Disk Failure ITIL: NetApp Filer Disk Missing ITIL: NetApp Filer File System Full ITIL: NetApp Filer RAID Disk Inserted ITIL: NetApp Filer RAID Disk Pulled ITIL: NetApp Filer Snapshot Error

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
		ITIL: NTP Server Unreachable
Availability Management	LogLogic LMI solution, in conjunction with the TIBCO LogLogic® Compliance Suite - ITIL Edition, provides the reports and alerts around which a variety of daily security operational procedures can be built or improved.	**Compliance Suite Reports** (Cont.) ITIL: PANOS: Attacks by Event ID ITIL: PANOS: Attacks by Threat Name ITIL: PANOS: Attacks Detected ITIL: Periodic Review of Log Reports ITIL: Pulse Connect Secure System Error ITIL: Symantec AntiVirus: Attacks by Threat Name ITIL: Symantec AntiVirus: Attacks Detected ITIL: Symantec AntiVirus: Scans ITIL: Symantec Endpoint Protection: Attacks by Threat Name ITIL: Symantec Endpoint Protection: Attacks Detected ITIL: Symantec Endpoint Protection: Scans ITIL: TrendMicro OfficeScan: Attacks Detected ITIL: TrendMicro OfficeScan: Attacks Detected by Threat Name ITIL: TrendMicro Control Manager: Attacks Detected ITIL: TrendMicro Control Manager: Attacks Detected by Threat Name ITIL: Windows AD Backup Error ITIL: Windows AD Backup Failed ITIL: Windows AD Backup Starting ITIL: Windows AD Exception Errors ITIL: Windows AD Replication Error ITIL: Windows AD Restore Failed ITIL: Windows AD Unable to Recover **Compliance Suite Alerts** ITIL: Cisco PIX, ASA, FWSM Failover Disabled ITIL: Cisco PIX, ASA, FWSM Failover Errors ITIL: Cisco PIX, ASA, FWSM Failover Performed ITIL: Cisco Switch Interface Down ITIL: Cisco Switch Interface Up ITIL: Juniper Firewall HA State Change

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
Availability Management	LogLogic LMI solution, in conjunction with the TIBCO LogLogic® Compliance Suite - ITIL Edition, provides the reports and alerts around which a variety of daily security operational procedures can be built or improved.	**Compliance Suite Alerts** (Cont.) ITIL: Juniper VPN System Error ITIL: LogLogic Disk Full ITIL: LogLogic HA State Change ITIL: LogLogic Management Center Backed Up or Restored ITIL: NetApp Filer Backup Errors ITIL: NetApp Filer Disk Failure ITIL: NetApp Filer Disk Inserted ITIL: NetApp Filer Disk Missing ITIL: NetApp Filer Disk Pulled ITIL: NetApp Filer File System Full ITIL: NetApp Filer Snapshot Error ITIL: NTP Server Unreachable ITIL: VPN Connection Capacity Exceeded ITIL: Windows AD Backup Error ITIL: Windows AD Backup Failed ITIL: Windows AD Backup Starting ITIL: Windows AD Replication Error ITIL: Windows AD Restore Failed
Service Support		

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
Incident Management	LogLogic LMI solution, in conjunction with the TIBCO LogLogic® Compliance Suite - ITIL Edition, provides the reports and alerts around which a variety of daily security operational procedures can be built or improved.	**Compliance Suite Reports** ITIL: Cisco PIX, ASA, FWSM Failover Errors ITIL: Cisco PIX, ASA, FWSM Failover Performed ITIL: Cisco PIX, ASA, FWSM Restarted ITIL: Cisco PIX, ASA, FWSM Routing Failure ITIL: Cisco Routers and Switches Restart ITIL: Cisco Switch Interface Down ITIL: Cisco Switch Interface Up ITIL: DNS Server Error ITIL: FireEye MPS: Attacks by Event ID ITIL: FireEye MPS: Attacks by Threat Name ITIL: FireEye MPS: Attacks Detected ITIL: F5 BIG-IP TMOS Restarted ITIL: i5/OS Restarted ITIL: Juniper Firewall HA State Changed ITIL: Juniper Firewall Policy Out of Sync ITIL: Juniper Firewall Reset Accepted ITIL: Juniper Firewall Reset Imminent ITIL: Juniper Firewall Restarted ITIL: LogLogic Disk Full ITIL: LogLogic HA State Changed ITIL: LogLogic Management Center Backup Activities ITIL: LogLogic Management Center Restore Activities ITIL: Microsoft Operations Manager - Windows Server Restarted ITIL: NetApp Filer Disk Failure ITIL: NetApp Filer Disk Missing ITIL: NetApp Filer File System Full ITIL: NetApp Filer RAID Disk Pulled ITIL: NetApp Filer Snapshot Error ITIL: NTP Daemon Exited ITIL: NTP Server Unreachable ITIL: Periodic Review of Log Reports ITIL: System Restarted

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
		ITIL: vCenter Orchestrator Virtual Machine Shutdown ITIL: vCenter Orchestrator Virtual Machine Started

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
Incident Management	LogLogic LMI solution, in conjunction with the TIBCO LogLogic® Compliance Suite - ITIL Edition, provides the reports and alerts around which a variety of daily security operational procedures can be built or improved.	**Compliance Suite Reports** (Cont.) ITIL: vCenter Shutdown or Restart of ESX Server ITIL: vCenter Virtual Machine Shutdown ITIL: vCenter Virtual Machine Started ITIL: Windows AD Backup Error ITIL: Windows AD Backup Failed ITIL: Windows AD Exception Errors ITIL: Windows AD Replication Error ITIL: Windows AD Restore Failed ITIL: Windows AD Startup ITIL: Windows AD Unable to Recover ITIL: Windows Servers Restarted ITIL: Windows Software Update Failures **Compliance Suite Alerts** ITIL: Cisco PIX, ASA, FWSM Failover Errors ITIL: System Restarted ITIL: Cisco PIX, ASA, FWSM Routing Failure ITIL: Cisco Routers and Switches Restarted ITIL: Cisco Switch Interface Down ITIL: Cisco Switch Interface Up ITIL: DNS Server Shutdown ITIL: DNS Server Started ITIL: Juniper Firewall HA State Change ITIL: Juniper Firewall Policy Out of Sync ITIL: Juniper Firewall Reset Imminent ITIL: Juniper Firewall System Reset ITIL: Juniper VPN System Error ITIL: LogLogic Disk Full ITIL: LogLogic HA State Change ITIL: LogLogic Management Center Backed Up or Restored ITIL: NetApp Filer Backup Errors ITIL: NetApp Filer Disk Failure ITIL: NetApp Filer Disk Missing ITIL: NetApp Filer Disk Pulled

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
Incident Management	LogLogic LMI solution, in conjunction with the TIBCO LogLogic® Compliance Suite - ITIL Edition, provides the reports and alerts around which a variety of daily security operational procedures can be built or improved.	**Compliance Suite Alerts** (Cont.) ITIL: NetApp Filer File System Full ITIL: NetApp Filer Snapshot Error ITIL: NTP Daemon Exited ITIL: NTP Server Unreachable ITIL: Pulse Connect Secure System Error ITIL: System Restarted ITIL: vCenter Orchestrator Virtual Machine Shutdown ITIL: vCenter Orchestrator Virtual Machine Started ITIL: vCenter Shutdown or Restart ESX ITIL: vCenter Virtual Machine Shutdown ITIL: vCenter Virtual Machine Started ITIL: Windows AD Backup Error ITIL: Windows AD Backup Failed ITIL: Windows AD Replication Error ITIL: Windows AD Restore Failed ITIL: Windows AD Startup ITIL: System Restarted

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
Problem Management	LogLogic LMI solution, in conjunction with the TIBCO LogLogic® Compliance Suite - ITIL Edition, provides the reports and alerts around which a variety of daily security operational procedures can be built or improved.	**Compliance Suite Reports** ITIL: Active Directory System Changes ITIL: Check Point Configuration Changes ITIL: Cisco ISE, ACS Configuration Changes ITIL: Cisco PIX, ASA, FWSM Failover Disabled ITIL: Cisco PIX, ASA, FWSM Failover Errors ITIL: Cisco PIX, ASA, FWSM Failover Performed ITIL: Cisco PIX, ASA, FWSM Policy Changed ITIL: Cisco PIX, ASA, FWSM Routing Failure ITIL: Cisco Switch Interface Down ITIL: Cisco Switch Interface Up ITIL: Cisco Switch Policy Changes ITIL: DNS Server Error ITIL: Domain activities on Symantec Endpoint Protection ITIL: Email Domains Experiencing Delay - Exchange 2000/2003 ITIL: ESX Kernel log daemon terminating ITIL: ESX Kernel logging Stop ITIL: ESX Syslogd Restart ITIL: HP NonStop Audit Configuration Changes ITIL: HP NonStop Audit Object Changes ITIL: HP NonStop Audit Permissions Changed ITIL: i5/OS Object Permissions Modified ITIL: i5/OS Service Started ITIL: Juniper Firewall HA State Changed ITIL: Juniper Firewall Policy Changed ITIL: Juniper Firewall Policy Out of Sync ITIL: LogLogic Disk Full ITIL: LogLogic HA State Changed ITIL: LogLogic Management Center Backup Activities ITIL: LogLogic Management Center Restore Activities ITIL: LogLogic Management Center Upgrade Success

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
		ITIL: LogLogic Universal Collector Configuration Changes ITIL: Microsoft Operations Manager - Windows Permissions Modified

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
Problem Management	LogLogic LMI solution, in conjunction with the TIBCO LogLogic® Compliance Suite - ITIL Edition, provides the reports and alerts around which a variety of daily security operational procedures can be built or improved.	**Compliance Suite Reports** (Cont.) ITIL: Microsoft Operations Manager - Windows Policies Modified ITIL: Microsoft Sharepoint Permissions Changed ITIL: Microsoft Sharepoint Policy Add, Remove, or Modify ITIL: NetApp Filer Disk Missing ITIL: NetApp Filer File System Full ITIL: NetApp Filer RAID Disk Inserted ITIL: NetApp Filer RAID Disk Pulled ITIL: NetApp Filer Snapshot Error ITIL: NetApp Filer Audit Policies Modified ITIL: NetApp Filer Boot Block Updated ITIL: NetApp Filer Disk Failure ITIL: NTP Daemon Exited ITIL: NTP Server Unreachable ITIL: Periodic Review of Log Reports ITIL: Permissions Modified on Windows Servers ITIL: Policies Modified on Windows Servers ITIL: RACF Permissions Changed ITIL: RACF Process Started ITIL: Software Update Successes on i5/OS ITIL: Symantec AntiVirus: Updated ITIL: Symantec Endpoint Protection Configuration Changes ITIL: Symantec Endpoint Protection Policy Add, Remove, or Modify ITIL: Symantec Endpoint Protection: Updated ITIL: TIBCO Administrator Permission Changes ITIL: TIBCO ActiveMatrix Administrator Permission Changes ITIL: vCenter Change Attributes ITIL: vCenter Modify Firewall Policy ITIL: vCenter Orchestrator Change Attributes ITIL: vCenter Orchestrator Virtual Machine Created

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
		ITIL: vCenter Orchestrator Virtual Machine Deleted

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
Problem Management	LogLogic LMI solution, in conjunction with the TIBCO LogLogic® Compliance Suite - ITIL Edition, provides the reports and alerts around which a variety of daily security operational procedures can be built or improved.	**Compliance Suite Reports** (Cont.) ITIL: vCenter Orchestrator vSwitch Added, Changed or Removed ITIL: vCenter Resource Usage Change ITIL: vCenter Restart ESX Services ITIL: vCenter User Permission Change ITIL: vCenter Virtual Machine Created ITIL: vCenter Virtual Machine Deleted ITIL: vCenter vSwitch Added, Changed or Removed ITIL: vCloud Organization Created ITIL: vCloud Organization Deleted ITIL: vCloud Organization Modified ITIL: vCloud vApp Created, Modified, or Deleted ITIL: vCloud vDC Created, Modified, or Deleted ITIL: vShield Edge Configuration Changes ITIL: Windows AD Backup Error ITIL: Windows AD Backup Failed ITIL: Windows AD Exception Errors ITIL: Windows AD Replication Error ITIL: Windows AD Restore Failed ITIL: Windows AD Unable to Recover ITIL: Windows Domain Activities ITIL: Windows New Services Installed ITIL: Windows Software Update Successes **Compliance Suite Alerts** ITIL: Active Directory Changes ITIL: Check Point Policy Changed ITIL: Cisco ISE, ACS Configuration Changed ITIL: Cisco PIX, ASA, FWSM Failover Disabled ITIL: Cisco PIX, ASA, FWSM Failover Errors ITIL: Cisco PIX, ASA, FWSM Failover Performed ITIL: Cisco PIX, ASA, FWSM Policy Changed ITIL: Cisco PIX, ASA, FWSM Routing Failure ITIL: Cisco PIX, ASA, FWSM Shun Added ITIL: Cisco PIX, ASA, FWSM Shun Deleted

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
		ITIL: Cisco Switch Interface Down

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
Problem Management	LogLogic LMI solution, in conjunction with the TIBCO LogLogic® Compliance Suite - ITIL Edition, provides the reports and alerts around which a variety of daily security operational procedures can be built or improved.	**Compliance Suite Alerts** (Cont.) ITIL: Cisco Switch Interface Up ITIL: Cisco Switch Policy Changed ITIL: HP NonStop Audit Configuration Changed ITIL: HP NonStop Audit Permission Changed ITIL: i5/OS Server or Service Status Change ITIL: Juniper Firewall HA State Change ITIL: Juniper Firewall Policy Changes ITIL: Juniper Firewall Policy Out of Sync ITIL: Juniper VPN Policy Change ITIL: Juniper VPN System Error ITIL: LogLogic Disk Full ITIL: LogLogic HA State Change ITIL: LogLogic Management Center Backed Up or Restored ITIL: LogLogic Management Center Upgrade Succeeded ITIL: LogLogic Universal Collector Configuration Changed ITIL: Microsoft Operations Manager - Permissions Changed ITIL: Microsoft Operations Manager - Windows Policies Changed ITIL: Microsoft Sharepoint Permission Changed ITIL: Microsoft Sharepoint Policies Added, Removed, Modified ITIL: NetApp Filer Audit Policies Changed ITIL: NetApp Filer Backup Errors ITIL: NetApp Bootblock Update ITIL: NetApp Filer Disk Failure ITIL: NetApp Filer Disk Inserted ITIL: NetApp Filer Disk Missing ITIL: NetApp Filer Disk Pulled ITIL: NetApp Filer File System Full ITIL: NetApp Filer Snapshot Error ITIL: NTP Daemon Exited ITIL: NTP Server Unreachable

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
Problem Management	LogLogic LMI solution, in conjunction with the TIBCO LogLogic® Compliance Suite - ITIL Edition, provides the reports and alerts around which a variety of daily security operational procedures can be built or improved.	**Compliance Suite Alerts** (Cont.) ITIL: Pulse Connect Secure System Error ITIL: Pulse Connect Secure Policy Change ITIL: RACF Permissions Changed ITIL: RACF Process Started ITIL: Symantec Endpoint Protection Configuration Changed ITIL: Symantec Endpoint Protection Domains Created ITIL: Symantec Endpoint Protection Policy Add, Delete, Modify ITIL: TIBCO ActiveMatrix Administrator Permission Changed ITIL: vCenter Create Virtual Machine ITIL: vCenter Delete Virtual Machine ITIL: vCenter Firewall Policy Change ITIL: vCenter Orchestrator Create Virtual Machine ITIL: vCenter Orchestrator Delete Virtual Machine ITIL: vCenter Orchestrator vSwitch Add, Modify or Delete ITIL: vCenter Permission Change ITIL: vCenter Restart ESX Services ITIL: vCenter vSwitch Add, Modify or Delete ITIL: vCloud Organization Created ITIL: vCloud Organization Deleted ITIL: vCloud Organization Modified ITIL: vCloud User, Group, or Role Modified ITIL: vCloud vApp Created, Deleted, or Modified ITIL: vCloud vDC Created, Modified, or Deleted ITIL: vShield Edge Configuration Change ITIL: Windows AD Backup Error ITIL: Windows AD Backup Failed ITIL: Windows AD Replication Error ITIL: Windows AD Restore Failed ITIL: Windows Domains Created ITIL: Windows New Services Installed ITIL: Windows Permissions Changed

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
		ITIL: Windows Policies Changed ITIL: Windows Software Updates

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
Configuration Management	LogLogic LMI solution, in conjunction with the TIBCO LogLogic® Compliance Suite - ITIL Edition, provides the reports and alerts around which a variety of daily security operational procedures can be built or improved.	**Compliance Suite Reports** ITIL: Active Directory System Changes ITIL: Check Point Configuration Changes ITIL: Cisco ISE, ACS Configuration Changes ITIL: Cisco PIX, ASA, FWSM Failover Disabled ITIL: Cisco PIX, ASA, FWSM Policy Changed ITIL: Cisco Switch Policy Changes ITIL: ESX Kernel log daemon terminating ITIL: ESX Kernel logging Stop ITIL: ESX Syslogd Restart ITIL: HP NonStop Audit Configuration Changes ITIL: HP NonStop Audit Object Changes ITIL: HP NonStop Audit Permissions Changed ITIL: i5/OS Object Permissions Modified ITIL: i5/OS Service Started ITIL: Juniper Firewall Policy Changed ITIL: LogLogic Universal Collector Configuration Changes ITIL: Microsoft Operations Manager - Windows Permissions Modified ITIL: Microsoft Operations Manager - Windows Policies Modified ITIL: Microsoft Sharepoint Permissions Changed ITIL: Microsoft Sharepoint Policy Add, Remove, or Modify ITIL: NetApp Filer Audit Policies Modified ITIL: Permissions Modified on Windows Servers ITIL: Periodic Review of Log Reports ITIL: Policies Modified on Windows Servers ITIL: RACF Permissions Changed ITIL: RACF Process Started ITIL: Symantec AntiVirus: Updated ITIL: Symantec Endpoint Protection Configuration Changes ITIL: Symantec Endpoint Protection Policy Add, Remove, or Modify ITIL: Symantec Endpoint Protection: Updated

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
Configuration Management	LogLogic LMI solution, in conjunction with the TIBCO LogLogic® Compliance Suite - ITIL Edition, provides the reports and alerts around which a variety of daily security operational procedures can be built or improved.	**Compliance Suite Reports** (Cont.) ITIL: TIBCO Administrator Permission Changes ITIL: TIBCO ActiveMatrix Administrator Permission Changes ITIL: vCenter Change Attributes ITIL: vCenter Modify Firewall Policy ITIL: vCenter Orchestrator Change Attributes ITIL: vCenter Orchestrator Virtual Machine Created ITIL: vCenter Orchestrator Virtual Machine Deleted ITIL: vCenter Orchestrator vSwitch Added, Changed or Removed ITIL: vCenter Resource Usage Change ITIL: vCenter Restart ESX Services ITIL: vCenter User Permission Change ITIL: vCenter Virtual Machine Created ITIL: vCenter Virtual Machine Deleted ITIL: vCenter vSwitch Added, Changed or Removed ITIL: vCloud Organization Created ITIL: vCloud Organization Deleted ITIL: vCloud Organization Modified ITIL: vCloud vApp Created, Modified, or Deleted ITIL: vCloud vDC Created, Modified, or Deleted ITIL: vShield Edge Configuration Changes ITIL: Windows New Services Installed **Compliance Suite Alerts** ITIL: Active Directory Changes ITIL: Check Point Policy Changed ITIL: Cisco ISE, ACS Configuration Changed ITIL: Cisco PIX, ASA, FWSM Failover Disabled ITIL: Cisco PIX, ASA, FWSM Policy Changed ITIL: Cisco PIX, ASA, FWSM Shun Added ITIL: Cisco PIX, ASA, FWSM Shun Deleted ITIL: Cisco Switch Policy Changed ITIL: HP NonStop Audit Configuration Changed

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
		ITIL: HP NonStop Audit Permission Changed

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
Configuration Management	LogLogic LMI solution, in conjunction with the TIBCO LogLogic® Compliance Suite - ITIL Edition, provides the reports and alerts around which a variety of daily security operational procedures can be built or improved.	**Compliance Suite Alerts** (Cont.) ITIL: i5/OS Server or Service Status Change ITIL: Juniper Firewall Policy Changes ITIL: Juniper VPN Policy Change ITIL: LogLogic Universal Collector Configuration Changed ITIL: Microsoft Operations Manager - Permissions Changed ITIL: Microsoft Operations Manager - Windows Policies Changed ITIL: Microsoft Sharepoint Permission Changed ITIL: Microsoft Sharepoint Policies Added, Removed, Modified ITIL: NetApp Filer Audit Policies Changed ITIL: Pulse Connect Secure Policy Change ITIL: RACF Permissions Changed ITIL: RACF Process Started ITIL: Symantec Endpoint Protection Configuration Changed ITIL: Symantec Endpoint Protection Domains Created ITIL: Symantec Endpoint Protection Policy Add, Delete, Modify ITIL: TIBCO ActiveMatrix Administrator Permission Changed ITIL: vCenter Create Virtual Machine ITIL: vCenter Delete Virtual Machine ITIL: vCenter Firewall Policy Change ITIL: vCenter Orchestrator Create Virtual Machine ITIL: vCenter Orchestrator Delete Virtual Machine ITIL: vCenter Orchestrator vSwitch Add, Modify or Delete ITIL: vCenter Permission Change ITIL: vCenter Restart ESX Services ITIL: vCenter vSwitch Add, Modify or Delete ITIL: vCloud Organization Created ITIL: vCloud Organization Deleted ITIL: vCloud Organization Modified

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
		ITIL: vCloud User, Group, or Role Modified
Configuration Management	LogLogic LMI solution, in conjunction with the TIBCO LogLogic® Compliance Suite - ITIL Edition, provides the reports and alerts around which a variety of daily security operational procedures can be built or improved.	**Compliance Suite Alerts** (Cont.) ITIL: vCloud vApp Created, Deleted, or Modified ITIL: vCloud vDC Created, Modified, or Deleted ITIL: vShield Edge Configuration Change ITIL: Windows Domains Created ITIL: Windows New Services Installed ITIL: Windows Permissions Changed ITIL: Windows Policies Changed ITIL: Windows Software Updates

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
Change Management	LogLogic LMI solution, in conjunction with the TIBCO LogLogic® Compliance Suite - ITIL Edition, provides the reports and alerts around which a variety of daily security operational procedures can be built or improved.	**Compliance Suite Reports** ITIL: Active Directory System Changes ITIL: Check Point Configuration Changes ITIL: Cisco ISE, ACS Configuration Changes ITIL: Cisco PIX, ASA, FWSM Failover Disabled ITIL: Cisco PIX, ASA, FWSM Policy Changed ITIL: Cisco Switch Policy Changes ITIL: ESX Kernel log daemon terminating ITIL: ESX Kernel logging Stop ITIL: ESX Syslogd Restart ITIL: HP NonStop Audit Configuration Changes ITIL: HP NonStop Audit Object Changes ITIL: HP NonStop Audit Permissions Changed ITIL: i5/OS Object Permissions Modified ITIL: i5/OS Service Started ITIL: Juniper Firewall Policy Changed ITIL: LogLogic Management Center Upgrade Success ITIL: LogLogic Universal Collector Configuration Changes ITIL: Microsoft Operations Manager - Windows Permissions Modified ITIL: Microsoft Operations Manager - Windows Policies Modified ITIL: Microsoft Sharepoint Permissions Changed ITIL: Microsoft Sharepoint Policy Add, Remove, or Modify ITIL: NetApp Filer Audit Policies Modified ITIL: NetApp Filer RAID Disk Inserted ITIL: NetApp Filer RAID Disk Pulled ITIL: Periodic Review of Log Reports ITIL: RACF Permissions Changed ITIL: RACF Process Started ITIL: Software Update Successes on i5/OS ITIL: Symantec AntiVirus: Updated ITIL: Symantec Endpoint Protection Configuration Changes

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
Change Management	LogLogic LMI solution, in conjunction with the TIBCO LogLogic® Compliance Suite - ITIL Edition, provides the reports and alerts around which a variety of daily security operational procedures can be built or improved.	**Compliance Suite Reports** (Cont.) ITIL: Symantec Endpoint Protection Policy Add, Remove, or Modify ITIL: Symantec Endpoint Protection: Updated ITIL: TIBCO Administrator Permission Changes ITIL: TIBCO ActiveMatrix Administrator Permission Changes ITIL: vCenter Change Attributes ITIL: vCenter Modify Firewall Policy ITIL: vCenter Orchestrator Change Attributes ITIL: vCenter Orchestrator Virtual Machine Created ITIL: vCenter Orchestrator Virtual Machine Deleted ITIL: vCenter Orchestrator vSwitch Added, Changed or Removed ITIL: vCenter Resource Usage Change ITIL: vCenter Restart ESX Services ITIL: vCenter User Permission Change ITIL: vCenter Virtual Machine Created ITIL: vCenter Virtual Machine Deleted ITIL: vCenter vSwitch Added, Changed or Removed ITIL: vCloud Organization Created ITIL: vCloud Organization Deleted ITIL: vCloud Organization Modified ITIL: vCloud vApp Created, Modified, or Deleted ITIL: vCloud vDC Created, Modified, or Deleted ITIL: vShield Edge Configuration Changes ITIL: Windows New Services Installed ITIL: Permissions Modified on Windows Servers ITIL: Policies Modified on Windows Servers ITIL: Windows Software Update Successes **Compliance Suite Alerts** ITIL: Active Directory Changes ITIL: Check Point Policy Changed ITIL: Cisco ISE, ACS Configuration Changed

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
		ITIL: Cisco PIX, ASA, FWSM Failover Disabled ITIL: Cisco PIX, ASA, FWSM Policy Changed

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
Change Management	LogLogic LMI solution, in conjunction with the TIBCO LogLogic® Compliance Suite - ITIL Edition, provides the reports and alerts around which a variety of daily security operational procedures can be built or improved.	**Compliance Suite Alerts** (Cont.) ITIL: Cisco PIX, ASA, FWSM Shun Added ITIL: i5/OS Server or Service Status Change ITIL: Cisco PIX, ASA, FWSM Shun Deleted ITIL: Cisco Switch Policy Changed ITIL: HP NonStop Audit Configuration Changed ITIL: HP NonStop Audit Permission Changed ITIL: Juniper Firewall Policy Changes ITIL: Juniper VPN Policy Change ITIL: LogLogic Management Center Upgrade Succeeded ITIL: LogLogic Universal Collector Configuration Changed ITIL: Microsoft Operations Manager - Permissions Changed ITIL: Microsoft Operations Manager - Windows Policies Changed ITIL: Microsoft Sharepoint Permission Changed ITIL: Microsoft Sharepoint Policies Added, Removed, Modified ITIL: NetApp Filer Audit Policies Changed ITIL: NetApp Filer Disk Inserted ITIL: NetApp Filer Disk Pulled ITIL: Pulse Connect Secure Policy Change ITIL: RACF Permissions Changed ITIL: RACF Process Started ITIL: Symantec Endpoint Protection Configuration Changed ITIL: Symantec Endpoint Protection Domains Created ITIL: Symantec Endpoint Protection Policy Add, Delete, Modify ITIL: TIBCO ActiveMatrix Administrator Permission Changed ITIL: vCenter Create Virtual Machine ITIL: vCenter Delete Virtual Machine ITIL: vCenter Firewall Policy Change ITIL: vCenter Orchestrator Create Virtual Machine

Implementation Specification	Description	TIBCO LogLogic Reports and Alerts
Change Management	LogLogic LMI solution, in conjunction with the TIBCO LogLogic® Compliance Suite - ITIL Edition, provides the reports and alerts around which a variety of daily security operational procedures can be built or improved.	**Compliance Suite Alerts** (Cont.) ITIL: vCenter Orchestrator Delete Virtual Machine ITIL: vCenter Orchestrator vSwitch Add, Modify or Delete ITIL: vCenter Permission Change ITIL: vCenter Restart ESX Services ITIL: vCenter vSwitch Add, Modify or Delete ITIL: vCloud Organization Created ITIL: vCloud Organization Deleted ITIL: vCloud Organization Modified ITIL: vCloud User, Group, or Role Modified ITIL: vCloud vApp Created, Deleted, or Modified ITIL: vCloud vDC Created, Modified, or Deleted ITIL: vShield Edge Configuration Change ITIL: Windows Domains Created ITIL: Windows New Services Installed ITIL: Windows Permissions Changed ITIL: Windows Policies Changed ITIL: Windows Software Updates