Splunk

Contents

- 1 Introduction
- 2 Requirements
- 3 Installation
- 4 Splunk Syslog Configuration
- 5 Splunk XML Log File Configuration
- 6 Verifying the Installation
- 7 Additional Information

Introduction

This document outlines how to integrate Splunk with Swivel by using Syslog and/or PINsafe log files. The integration requires the PINsafe server to write log files to a location that can be read by the Splunk server.

Requirements

Swivel, running version 3.2 or later. (This article is based on Version 3.6 running on Windows XP)

Splunk server, (This article was based on Splunk running on Windows XP)

Installation

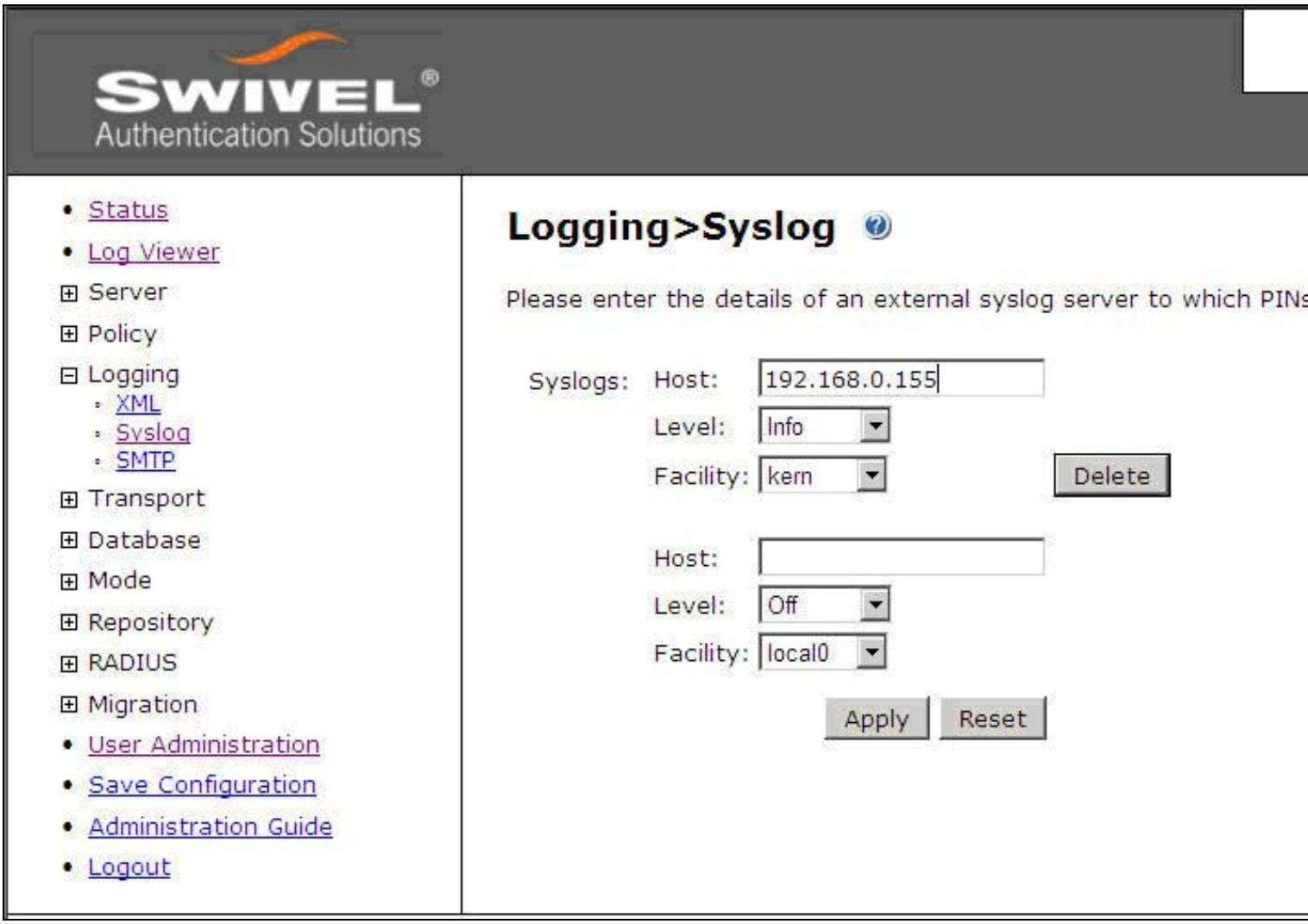
On the Swivel Administration Console, configure PINsafe to send syslog information to the Splunk server by selecting Logging/Syslog.

Enter the following information

Host: Hostname or IP address of the Splunk server

Level: The level of log information to be sent

Facility: The syslog facility in which event logs will be sent



If there is no syslog service, the PINsafe .xml log files produced by PINsafe can be imported into Splunk.

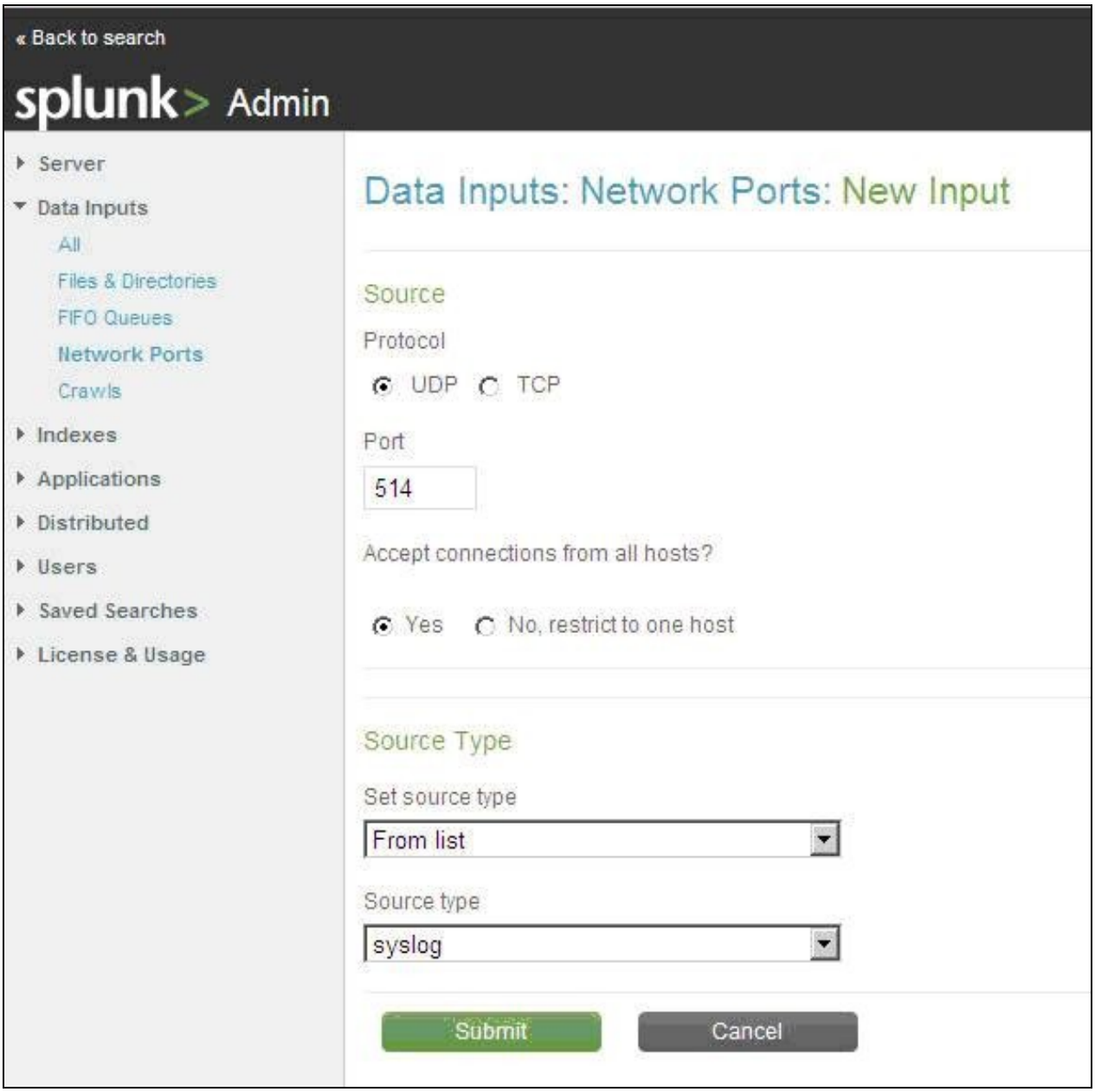
For a PINsafe appliance, they can be manually copied off to the Splunk server, see the appliance Administration guide for further details.

Alternatively a scheduled job maybe employed to copy the files across.

Splunk Syslog Configuration

On the Splunk server select Data Inputs/Network Ports then New Input, select the following options:

Source: UDP Port: 514 Accept connections from all hosts?: optional Set Source Type: From List Source Type: Syslog

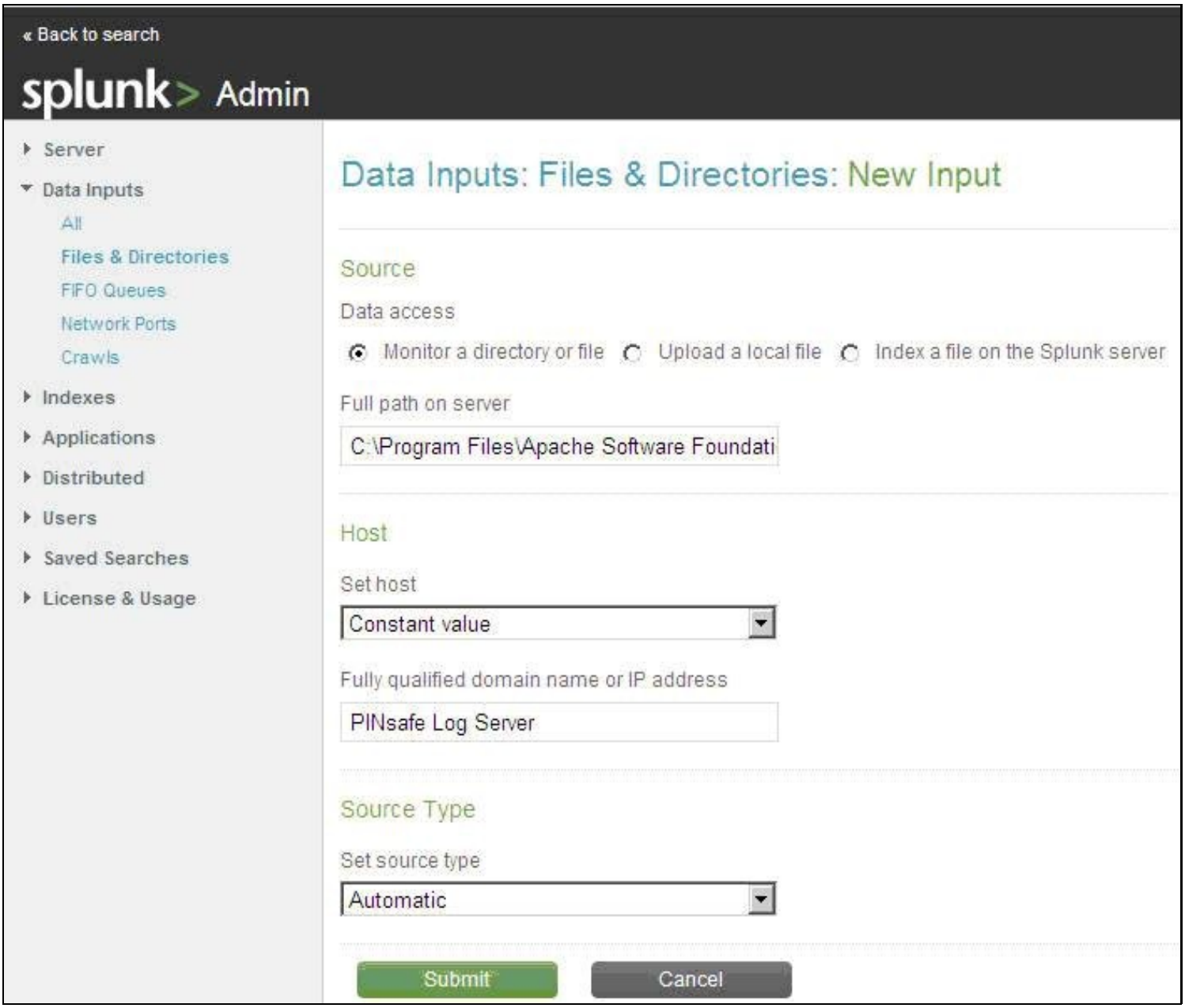


Then restart the Splunk Application by selecting Server/Control Server and Restart Now.

Splunk XML Log File Configuration

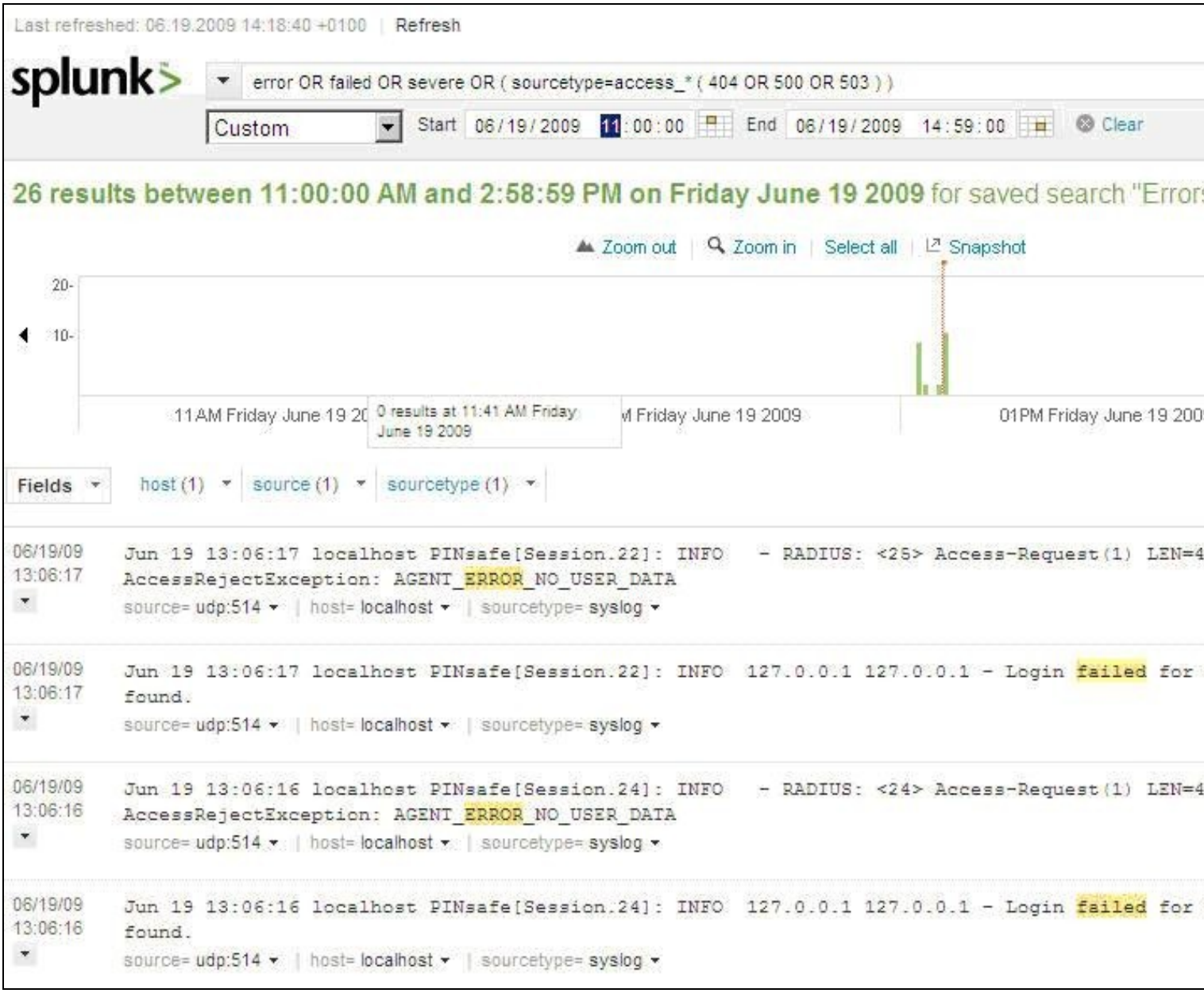
On the Splunk server select Data Inputs/Files and Directories then New Input, select the following options:

Data Access: Monitor a directory or file Full Path on server: location of log files Set Source Type: Automatic



Verifying the Installation

The Splunk screen should show input when PINsafe events occur or from historical logs.



These events can be filtered to display only specific events. Refer to Splunk documentation for more details.

Additional Information

For assistance in the PINsafe installation and configuration please firstly contact your reseller and then email Swivel Secure support at support@swivelsecure.com