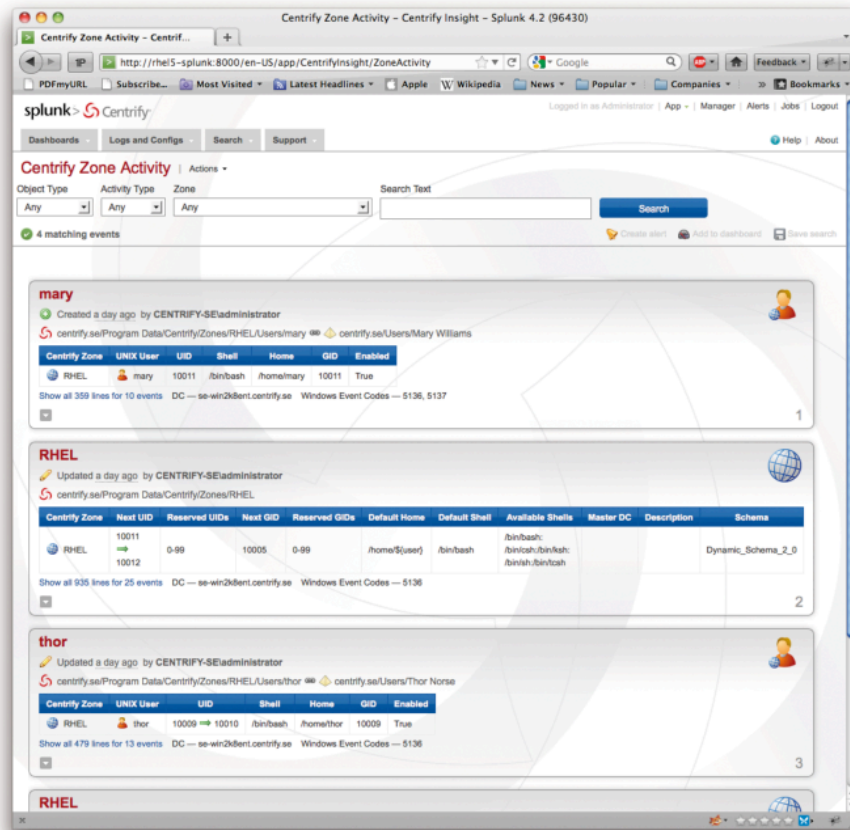# Splunk for Centrify Insight

Delivering the control, visibility and security of your cross-platform data center.

The Challenge

Heterogeneous IT environments have become the standard for both for server operating systems and the applications that run on them. With diverse operating systems and applications spanning physical, virtual and cloud-based environments, along with more Java- and web-based applications, the trend toward diversity is only accelerating.

Not surprisingly, interoperability among these diverse platforms is a key concern for IT managers. Reducing complexity has become even more critical in the past few years as an uncertain economy has put renewed focus on reducing expenses and leveraging existing investments.

Meanwhile, security and compliance have become even more critical as organizations cope with a dynamic business environment that includes mergers and acquisitions, staff reductions, and outsourcing.

The Solution

Splunk and Centrify can deliver the control and visibility you need to establish and manage the security of your cross-platform data center. You get a deeper insight into Active Directory status and the local system changes that affect the security and compliance of your environment.

Centrify Suite

The Centrify Suite lets you centrally control, secure and audit the access to your cross-platform systems and applications by leveraging your existing infrastructure—Active Directory. Built on an integrated architecture, the Centrify Suite enables organizations to strengthen security, enhance regulatory compliance initiatives, reduce IT expense and complexity and improve end-user productivity. The Centrify Suite—consisting of DirectControl, DirectAuthorize, DirectAudit, DirectSecure and DirectManage—delivers secure authentication and single sign-on, role-based access control, privileged identity management, user-level auditing, server isolation and encryption of data-in-motion for the industry's broadest set of heterogeneous systems and applications.

Splunk for Active Directory

Splunk is perfectly suited for monitoring and auditing Active Directory logs, because it matches the flexibility of Active Directory and can linearly scale as the Active Directory environment grows. Splunk can manage and analyze any data from any source type without requiring connectors. In addition, Splunk not only manages Active Directory's huge amount of data for trending and compliance requirements, it can also handle complex event processing for real-time monitoring and alerting.

Splunk for Active Directory is a pluggable data platform that provides visibility and control of highly complex Active Directory environments to system administrators and security specialists by aggregating, correlating and monitoring all security event logs and changes to AD schema.

Why Splunk for Centrify Insight

Centrify Suite can easily create reports that show what systems users have accessed and reveal their *NIX attributes. All of this information is centrally stored in Centrify Zones within Active Directory making it easy to manage and report. But wouldn't it
be great if you could also find out:

- Who Zone-enabled a user?

- When *NIX attribute(s) were changed?

- What Zone-groups have been modified?

- What changes were made to Active Directory Users, Groups and Computer objects?

Splunk for Centrify Insight App

With Centrify Insight powered by Splunk you can answer these types of historical questions and more. Centrify Insight is a Splunk application that listens to Active Directory domain controllers and security event logs, as well as *NIX syslog and Centrify Suite logs to provide the insight you need to answer security and forensic questions about Centrify secured systems. This data is captured and summarized into a series of reports and metrics that can be displayed, reported, alerted and analyzed at a granular level. Centrify Insight provide the visibility you need with an easy to use search interface and pre-built interactive reports based on the mature and popular Splunk platform. And best of all, Centrify is making this available for FREE!

About Splunk

Splunk is the engine for machine data. It is software which collects, indexes and harnesses any machine data generated by an organization's IT systems and infrastructure - physical, virtual and in the cloud. Machine data is unstructured, massive in scale and contains a categorical record of all transactions, systems, applications, user activities, security threats and fraudulent activity.

Splunk has the flexibility to collect all your data sources, the scalability to work across your entire infrastructure and the power to provide deep drilldown, statistical analysis and real-time, custom dashboards to anyone in your organization.
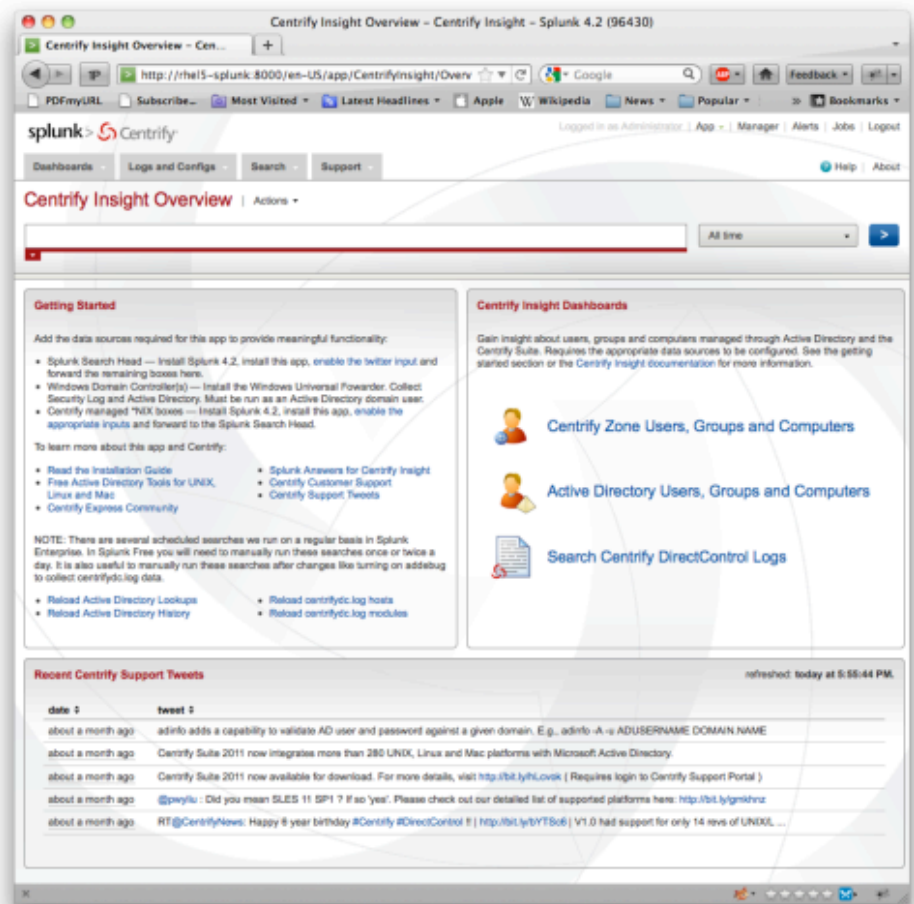
About Centrify

Centrify delivers integrated software solutions that centrally control, secure and audit access to cross-platform systems and applications using Microsoft Active Directory. Centrify is deployed in production on hundreds of thousands of mission critical servers. Over 3,000 organizations rely on Centrify's identity consolidation and privilege management solutions to reduce IT expenses, strengthen security and meet compliance requirements.

Get Started Today !

Splunk:

Website:	http://splunk-base.splunk.com/apps
Address:	250 Brannan St, San Francisco, CA, USA, 94107
Email:	info@splunk.com	sales@splunk.com
Phone:	+1 866-438-7758	+1 415-848-8400
Free Download:	www.splunk.com/download
More Info:	sales@splunk.com

Centrify:

Website:	http://www.centrify.com/splunk
Address:	785 Mary Ave, #200, Sunnyvale, CA USA
Email:	info@centrify.com
Phone:	+1 (408) 542-7500
Free Download:	http://www.centrify.com/try