SERVER SUITE TECHNICAL BRIEF

Configuring OpenSSH for Kerberos-Based Authentication to Linux & UNIX

How to implement Active Directory-based silent authentication for OpenSSH to AIX, HP-UX, Red Hat, Solaris, SUSE Ubuntu, VMware and other non-Windows systems using the Centrify Suite

SSH has become the de facto standard for administrators and users to securely access remote UNIX systems. The combination of the latest versions of OpenSSH supporting Kerberized connections, along with Certify Server Suite's ability to directly integrate UNIX and Linux computers with Active Directory's Kerberos infrastructure, provides system administrators with the ideal environment for secured single sign-on. They can log in from Windows using their Active Directory credentials and then automatically and yet securely access remote UNIX or Linux computers.

Centrify includes a Centrify-enabled version of OpenSSH free of charge with both the Centrify Server Suite and Centrify Express to help you be more productive and to accelerate your deployment.

You can download the Centrify-enabled version of OpenSSH along with Centrify Express, our free Active Directory-based solution for authentication and single sign-on to cross-platform systems.

Features & Benefits of the Centrify-Enabled OpenSSH

While many UNIX systems may have an sshd server installed, most will be older implementations of the sshd server that do not support Kerberos. Centrify provides a compiled version of the latest OpenSSH distribution to make it easier for you to install and use SSH with Server Suite for secured authentication via Kerberos to Active Directory.

Centrify has compiled the standard OpenSSH distribution unmodified, but in the compile process we linked OpenSSH with the Server Suite Kerberos libraries to ensure that single sign-on works seamlessly as expected in an Active Directory environment. This provides several advantages, including:

- The OpenSSH client and server are preconfigured to automatically support PAM and Kerberos.
- There is no need for DNS-to-realm mapping because Server Suite knows the relationship between hosts and their SPNs.
- There is no need for a .k5login file in the user's home directory since Server Suite can automatically map the UPN (User Principal Name) in the Kerberos ticket to the UNIX profile for the Active Directory username presented in the ticket.
- Server Suite will accept connections to any of the computer's valid hostnames, either fully qualified or not, because all combinations are registered with Active Directory. This further reduces the dependency on accurate DNS entries to enable Kerberos to operate properly.
- The installation process automatically updates the $PATH environment by adding /usr/share/centrifydc/bin for all users and /usr/share/centrifydc/sbin for administrators and super users, making direct access to OpenSSH possible.

Another advantage of Centrify-enabled OpenSSH is that it provides you a consistent and more up-to-date version of OpenSSH across your heterogeneous systems that are invariably running different versions of OpenSSH, including versions that may not have the latest security enhancements. For example, say you are running a mixed environment of Ubuntu 10.04, SUSE 11.2 and Fedora 13. That means you are running OpenSSH versions 5.3p1, 5.2p1 and 5.4p1 respectively. Centrify allows you to have a consistent and more up-to-date versions across your heterogeneous environment, that is also being continuously updated and fully supported by Centrify, which is another advantage.

That being said, Centrify provides Centrify-enabled OpenSSH as a convenience to you, but if you want to use the SSH provided by the OS vendor, or use a commercial SSH vendor, Centrify supports that too (and has fully tested our solution in all of these scenarios). Using our supplied OpenSSH is simply an installation choice, and not a

requirement. The bottom line is Centrify gives you choice - use the Centrify-enabled OpenSSH with the advantages noted above, the "stock" OpenSSH, or a commercial SSH solution - and Centrify works well with the choice you want. For example, here's a how to video on how to use Centrify Express with stock SSH. Centrify has found that most IT organizations prefer consistency across all their platforms, hence the value of getting an OpenSSH or Samba distribution from a single vendor who supports multiple platforms. In the case of OpenSSH from Centrify, this guarantees support for GSS Key Exchange on all platforms in order to establish trust between hosts, a feature which is not part of the standard OpenSSH distribution. But in the end it is your choice, and choice is good.

Contact Centrify

Centrify provides unified identity management across data center, cloud and mobile environments that result in single sign-on (SSO) for users and a simplified identity infrastructure for IT. Centrify's unified identity management software and cloud-based Identity-as-a-Service (IDaaS) solutions leverage an organization's existing identity infrastructure to enable single sign-on, multi-factor authentication, privileged identity management, auditing for compliance and enterprise mobility management.

Santa Clara, California:	+1 (669) 444-5200	Email	sales@centrify.com
EMEA:	+44 (0) 1344 317950	Web	http://www.centrify.com
Asia Pacific:	+61 1300 795 789		
Brazil:	+55 11 3958 4876		
Latin America:	+1 305 900 5354		