Enforcing Enterprise-out Security for Cloud Servers

By David McNeely

Cloud-based computing models offer the promise of a highly scalable compute infrastructure without having to acquire, install and maintain any additional hardware. However, implementing this new compute model using even the most trusted service providers requires a security solution that empowers IT to maintain control over user and network access to those hosted virtual machines. Security becomes even more important given the regulatory climate and audit pressures surrounding PCI, SOX, BASEL II and HIPAA. Centrify solves these difficult problems by providing an enterprise-out security enforcement approach that leverages existing Active Directory-based security policy enforcement and IPsec-based server and domain isolation. Together, these technologies enable rapid expansion of cloud compute capacity while still maintaining a secure environment.

Table of Contents

Introduction

The term Cloud Computing can mean many different things as there is a vast array of product and service offerings available on the market. Most analyst agree that there are three distinct types of Cloud Computing resources, Software as a Service (SaaS) with offerings such as WebEx or Salesforce.com, Platform as a Service (PaaS) with offerings such as Amazon CloudFront or Google App Engine and Infrastructure as a Service (IaaS) such as Amazon EC2 or Rackspace Cloud. These different service offerings appeal to different organizations within the Enterprise for

example the Sales organization may subscribe to Salesforce.com in order to use the hosted CRM functions of the service without having to worry about acquiring servers and software or building the solution in-house. In response to the increasingly dynamic needs of the business and ever increasing pressure to reduce costs, the hosted Infrastructure as a Service offerings have the potential to provide the Enterprise IT organization with infinitely expandable infrastructure on which to deliver their own services to the business. Irrespective of the business driver to leverage cloud computing systems, IT must ensure that any applications or services that they load on these hosted systems will be protected to the same and often higher standards than for existing internal applications.

There are several challenges that need to be to overcome before cloud systems can be integrated into the Enterprise. As new cloud servers are created and turned on, IT must take control over the current security configuration such as the privileged accounts and the security policies on the system. Additionally, IT needs to enable their own staff to be able to login using individual accounts with appropriate privileges for the duties for that person's role. Security policies need to be established that control access and ensure that only authorized users can access these systems. Once user access is under control, any user actions will need to be recorded in order to both provide visibility into the activities on these off-premise systems as well as to prove to auditors that these systems have adequate protections to meet regulatory requirements, such as PCI-DSS requirements for applications supporting online payment transactions. Ultimately, these systems are deployed in order to support an application providing service to the business. End users who access these systems and applications will need a simple way to gain access, ideally seamlessly accessing the application without having to login again if they have already logged into their desktop or laptop on the Enterprise network.

Centrify provides a comprehensive Enterprise security solution designed to automatically secure UNIX and Linux systems in order to enable their secured use in any environment including internal, Cloud and DMZ environments. Leveraging both Active Directory as well as IPsec based Server and Domain Isolation technologies for both Windows and UNIX/Linux systems enables secured use of these resources within Cloud environments. These systems are centrally secured, user access is controlled and they are isolated on the network from any untrusted communications. An Active Directory based security infrastructure additionally enables the Enterprise to leverage both existing IT processes such as account and security policy administration as well as to enable their existing users to access these new resources with their current Active Directory accounts. The resulting environment enables the organization to extend their computing infrastructure out to cloud based systems leveraging their existing security infrastructure based on Active Directory.

This document will provide guidance in five critical areas to address key security challenges that will help maximize success of cloud server projects by IT organizations:

- Automate Enterprise security controls on hosted systems

- Centralize account, access and privilege management

- Isolate hosted systems hardening network access

- Ensure visibility, accountability and audit on each system

- Provide Enterprise-centric Single Sign-on

Step 1. Automate Enterprise Security Controls on Hosted Systems

One of the first issues that needs to be addressed is based on the initial security settings embedded within the Cloud Servers that are typically created from templates provided by the service provider. These initial templates (for example, Amazon AMI images) will have a pre-defined security policy, which Enterprise IT must manage in order to establish their own security policies within the newly created cloud server. These pre-defined policies control several critical security settings such as who is allowed to authenticate, how they are allowed to access the system, which ports are accessible and most importantly how the privileged account is protected and who is allowed to run privileged commands.

IT could create their own cloud server templates in order to use servers that have an initial baseline state that complies with corporate standards. In many cases however, it may be simpler to leverage an existing pre-built server template since the Operating System vendor will keep these up to date with the latest release and patches. But, there needs to be a simple and automated way to take over the control of the security of these systems to enable usage of these pre-built server templates.

Automating Security Policy Enforcement

One of the primary benefits of cloud computing is the dynamic nature of the environment in which compute capacity can scale near infinitely to support the growing demands of the business. However, in order to secure these systems, the security infrastructure must also be automated in order to support the dynamic nature of these environments. For example, if a multi-tier customer facing application is deployed on a cloud infrastructure in order to take advantage of on-demand scaling based on demand, any new servers that are dynamically added to the application pool will need to be automatically secured as the instances are brought online and put into service. This scaling of an application can be quite dynamic and the security enforced will need to be inherently automatic to ensure that corporate security policies are enforced at all times.

Agent-based Enforcement of Centralized Policies

While there are many different methods an administrator may use to centrally define security policies through remote manipulation of each systems' locally defined security policies, Centrify uses an agent based model that establishes a centralized directory as the authoritative source for the security policies that should be enforced. Centrify Suite leverages Active Directory to manage a common set of security policies that will be dynamically enforced on each system as they join into the security environment. Once joined to Active Directory, Centrify DirectControl automatically enforces UNIX and Linux specific security policies, locking down privileged accounts and granting authorized access to the appropriate Active Directory user accounts. This agent based approach to security policy enforcement supports massive scalability unlike other central management server approaches due to the agent's local policy decision and policy enforcement based on a centralized and widely distributed trusted policy repository.
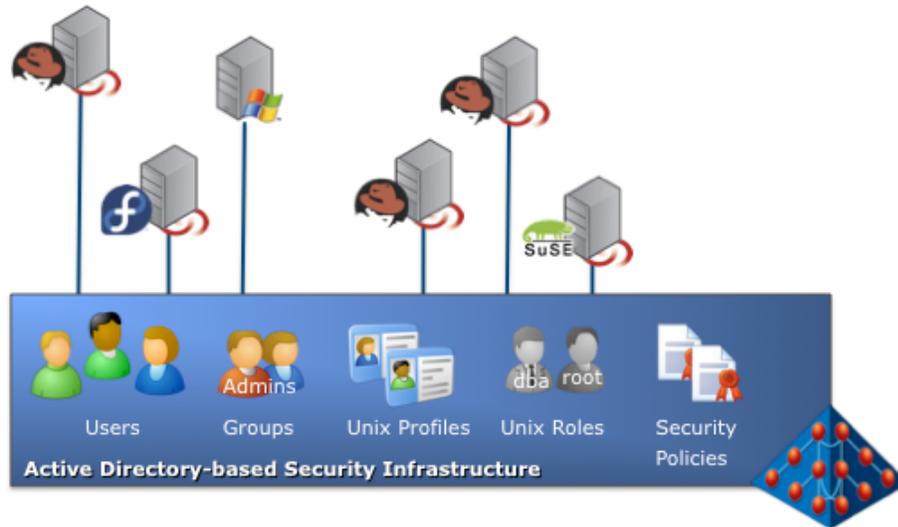
Figure 1: Cloud servers join Active Directory for enterprise security services

Cross-Forest Trust Leverages Existing User Accounts

In order to provide independent management of external resources and yet maintain the ability to enable the enterprise user to access these resources with their existing accounts leverages another key feature of Active Directory, cross-forest trust. A new Active Directory forest should be configured to provide security management for the DMZ and Cloud Servers with a one-way trust relationship to the internal Active Directory infrastructure where internal user accounts are managed. This configuration allows security policies to be managed independently from the hosting provider, as well as enabling management for both cloud- or extranet-based systems. Additionally, the trust relationship between the Active Directory Forests will enable internal users to leverage their existing credentials and desktop login to access hosted resources where specific permission has been granted.
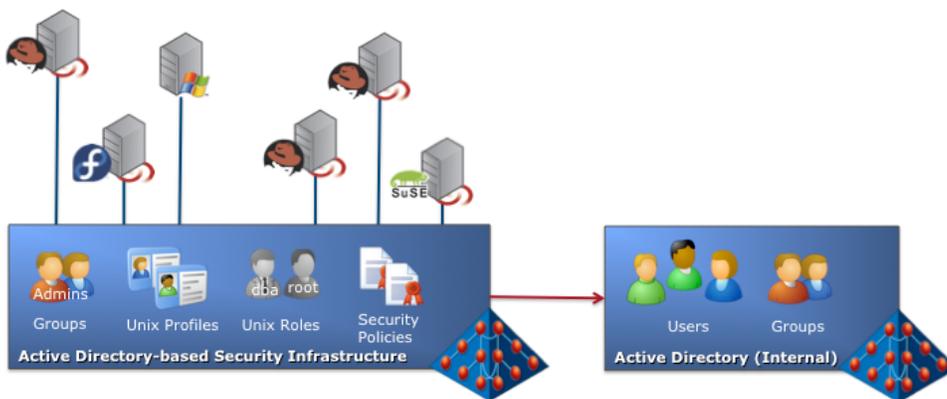

Figure 2: One-way cross-forest trust

Integration into Provisioning Process

Regardless of how the cloud server is provisioned, once the Active Directory infrastructure is in place and policies defined, all new cloud servers configured with Centrify Suite to join Active Directory will automatically enforce a

common security policy. Upon cloud server instance creation, either manually or through a provisioning system, the server is immediately joined to Active Directory through automated Centrify provisioning processes in order to establish a secured relationship between the new cloud server and the Active Directory domain. This provides the security foundation required to secure these new dynamic resources for production use.

Enforcing Enterprise Security Policies

Enterprise use of hosted systems requires enforcement of several security policies in order to ensure that Enterprise IT has proper controls over the access and use of those hosted systems, at least in those hosting environments where IT management has not been outsourced. Some of the more important security policies that should be defined and automatically enforced upon system join to Active Directory are listed below.

A trust relationship is established with the Active Directory

- Machine PKI certificate are automatically issued and renewed in order to provide a strong credential for trusted system identification.

System access security policies are centrally managed and locally enforced

- Host-based iptables firewall policies are enforced to block access to ports that should not be used based on the system's role.

- Host-based ipsec transport mode authentication, authorization and encryption policies are enforced to grant access to trusted systems as required by the system's role.

- OpenSSH security policies are enforced to deny root login and drop inactive sessions to ensure that only authorized users access the system.

Access and Privilege management is centrally controlled

- Service accounts such as root and oracle are linked to AD accounts for centralized management and password policy enforcement.

- Authorized users are granted access permissions and privileges as appropriate to their Role.

- Users are required to login with individual identities, preventing login with generic accounts to ensure accountability.

- Account management is centrally managed within AD to ensure proper access termination across all systems for users who no longer have a valid account.
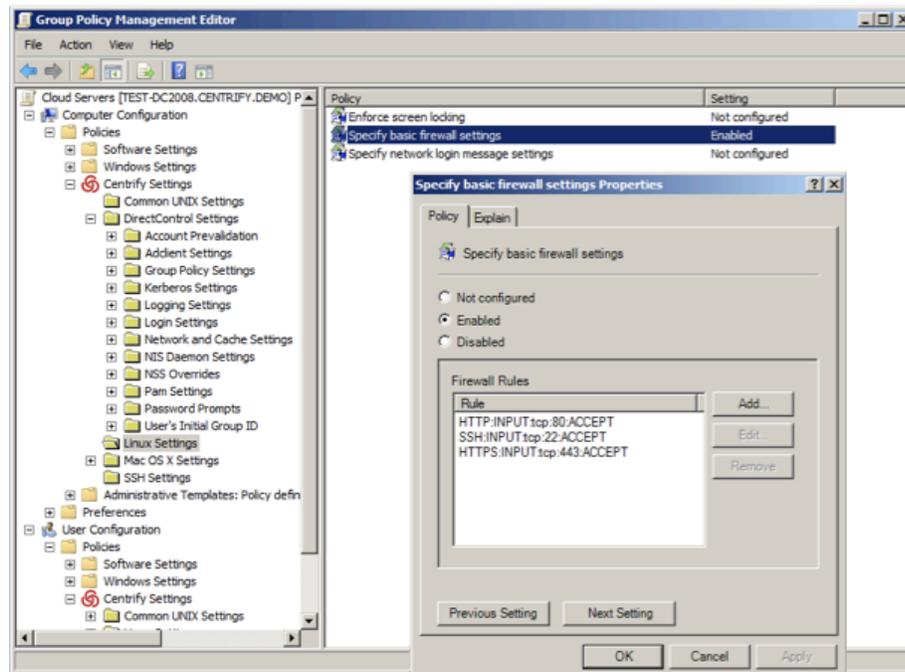
Figure 3: Group Policies are automatically enforced

The automated enforcement of all these policies provides an environment in which new systems can be brought online to provide additional capacity without worrying about the security of the overall environment, as each system will automatically enforce a common security policy. There is also no dependency upon a centralized configuration management process or server other than the availability of at least one Domain Controller to service the Domain to which these systems have been joined, and even this infrastructure has been designed to be highly fault tolerant, as most customers will deploy several servers for redundancy.

The benefit is that automated enforcement enables IT to focus on delivering highly scalable business services leveraging the elasticity of hosted compute environments with the assurance that business-critical security policies will be automatically enforced for every new system that is initialized into their cloud.

Step 2. Centralize Account, Access and Privilege Management

Cloud Servers are typically created and terminated dynamically based on workload of the overall system or application being deployed. This creates a highly dynamic life cycle where an identity and access management solution must also operate in an on-demand mode in order to enable IT Staff and End Users with appropriate access and privileges.

Take Over Control of Existing Privileged Accounts

The privileged account within each cloud server provides full control over the security of that server, therefore it is very important to take over control of these special accounts as soon as possible. Cloud servers are deployed by launching a copy of a server template or image, which will have a pre-defined root account and password and in

some cases another pre-defined user account that has full privileges on the system. In either case the Enterprise IT must take over control of these accounts since they have an initial password and security configuration that is common across the hosting environment, meaning that all other customers who use that image know the initial password.

Centrify Suite leverages both Active Directory and Zones to provide access control as well as a role-based privilege management model to ensure that the appropriate Enterprise users are granted access and privileges only where needed based on their role. In order to lock down existing local privileged accounts that are built into these cloud servers, Centrify provides a policy to map these local accounts to Active Directory accounts such that upon join to Active Directory the password will then become centrally managed. After the local privileged accounts have been linked to Active Directory, any attempts to login to these privileged accounts will require authentication using the password of the Active Directory account it is linked to. This policy enforcement then enables the Enterprise to take over control of the local privileged accounts automatically simply by joining the system to Active Directory where the Group Policies will be immediately applied to the system.
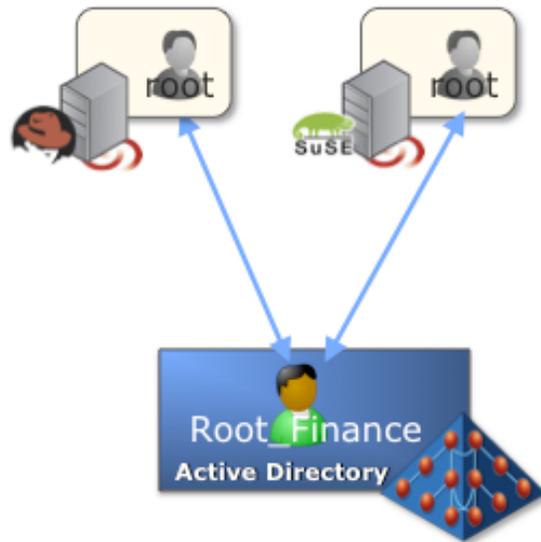

Figure 4: Mapping root to an Active Directory User account

Lockdown Privileged Access

Within some of the hosting environments that security policy controlling access to the privileged account is linked to an ssh key-based access control system as the root account does not have a password. In this model, the hosting provider has established a security policy to control access to any newly created cloud server instances by linking the server's ssh access control policy to the customer's account within the hosting environment so that a private key is required in order to access any servers created by the customer. This solution works quite well for smaller organizations where only a few administrators need to access the servers as they can simply share the ssh private keys. However in larger organizations with several administrators who need access, an access control or key management system is required in order to ensure that access can be controlled for each individual user.

Centrify provides a solution to lock down these privileged accounts as well as to control access at the SSH interface through tight integration with Active Directory. Through this integration with Active Directory and leveraging it's built-in Kerberos infrastructure, Centrify enables the use of Kerberos tickets for ssh clients to provide mutual authentication and enable authorized users to access the system seamlessly. An additional side benefit to the users who access the server is that if they have logged into their desktop workstation using their Active Directory credentials, they will be able to access the hosted servers without having to supply their userid or password, eg. single sign-on.

Grant Access Only to Authorized Users

In addition to taking control of the privileged accounts, it is important to ensure that users cannot log into the system with these privileged accounts and instead that they log into the system with their own individual account. These users will also need to be granted access based on the role of both the server as well as the user. For example if the server is providing database functions, then most likely the only users who need access are IT staff who provide support functions such as the system administrators, database administrators and help desk personnel. If the server is providing web services for an application, then both IT staff as well as end users will need various levels of access based on their role.

Centrify Suite leverages Active Directory user accounts as well as groups in order to manage the access controls for a given system or a group of systems also called a Zone. This model enables IT to leverage existing administrative processes in order to simplify the management of the access policies for these new resources. Additionally, one of the primary benefits of using the existing Active Directory infrastructure is the ability to leverage existing user account management processes such as new user account creation, password management, group membership and user account termination, all of which can be reused to control access to these new cloud servers.

Provide Privileges Based on Role

Most of the roles within IT will require some level of privileged access in order to carry out their duties on the servers that they are responsible for. While it is very common to simply grant full administrative rights to each person in IT, most of the job functions only require privileges to execute a limited set of commands. For example a web site administrator or developer will need elevated privileges in order to edit the web server configuration files and to start/stop/restart the web server, however he does not need full privileges that would enable him to create backdoor accounts or to change the firewall rules or other access controls on the server.

Ideally, each role within IT would be granted a specific set of privileges based on the job duties that are required. Then each person within IT would be assigned the appropriate privileges they require on the specific set of servers on which they need to work. While many organizations use sudo to provide privileges to the appropriate administrators, often it is used to grant full administrative privileges due to the difficulty of managing a more complex and granular policy. Centrify Suite provides both a centralized management for sudo based on Group Policy enforcement as well as DirectAuthorize which provides a more granular and dynamic privilege elevation solution. DirectAuthorize enforces a centralized policy held within Active Directory which defines which commands a specific Role is allowed to execute, which interfaces that Role is authorized to log into as well as restricting the shell via

white listed environment where necessary. Users or groups can be assigned these Roles as they grant privileges across individual computers or groups of computers on a permanent or temporary basis.

Figure 5: Privileges are granted to users and groups via Roles

The resulting environment enables centrally managed privileges to be granted to users in specific roles as they login to any of the newly created cloud servers that have joined Active Directory. This solution enables access and privilege management to be completely automated based on the new cloud server's trusted relationship with Active Directory, no other local system management is required in order to:

- take over the password for the local privileged accounts

- lock down privileged access

- require users to login with their own unique identities

- grant specific elevated privileges where required based on job duties

Step 3. Isolate Hosted Systems Hardening Network Access

There are many different hosting models available to choose from for Infrastructure as a Service ranging from virtual servers by the hour in a multi-tenant hosting environment to a virtual private data center in a dedicated hosting environment. With this wide range of offerings there are several different ways that these servers can be

inter-connected to the Enterprise. Typically the cloud servers will be assigned at least one private IP address to support communications between servers within the cloud and in many cases they will also be provided a public IP address. And since these servers are hosted in a multi-tenant environment, the Enterprise will need to provide additional controls to ensure that only authorized communication is allowed to these new servers. Centrify Suite provides automatic policy enforcement of firewall policies which are enforced on each new cloud server as it is created. Additionally, IT will need to ensure that any data in transit between these new cloud servers and any internal systems servers is protected. Centrify Suite also provides an identity-based server and domain isolation technology that enables secured peer-to-peer communications to be established between systems after authenticating each other via strong host-based credentials. This provides the foundation for hardening network access as well as ensuring that communications is only provided to trusted systems within the Enterprise.

Harden Network Access

Most hosting providers will enable IT to manage the security firewall rules that are provided within both the hosting environment as well as the host-based firewall built into the guest operating system. However, IT needs to ensure that these policies are managed and provide for adequate protection of the new cloud servers. Firewalls within the hosting environment are designed to enable the Enterprise to control which ports should or should not be accessible from outside the hosted guest server. These can provide the appropriate controls to prevent access on specific ports, but should not be trusted to grant limited access to the hosted system based on IP addresses in a virtualized environment. While hosting providers implement controls to prevent network scanning and spoofing of IP addressed, a stronger authentication mechanism is required to ensure that only trusted systems are able to communicate with servers holding more sensitive information. In order to provide impenetrable defenses on each of the guest servers, IPsec provides for authentication policies to control access to trusted systems such that only authenticated connections are allowed from other trusted systems. IPsec can be configured to require strong authentication using Kerberos tickets or PKI certificates for mutual authentication between trusted hosts.

Centrify Suite provides a Group Policy managed network security solution to both manage the built-in iptables-based firewall as well as the built-in IPsec stack on each of the hosted Linux servers. The iptables firewall Group Policy centralizes management of port level access controls to the hosted server, granting access to ports that should be open and denying access where those ports would pose a security risk. For communication ports that should only be used for private communications, IPsec is configured via Group Policy to provide server isolation that is interoperable with Microsoft Windows server and domain isolation security policies. This enables the Enterprise to define a common set of policies that both Windows and Linux will enforce, requiring mutual authentication of Enterprise issued strong credentials prior to network communications. This configuration will prevent communications from un-trusted systems since they will not be able to authenticate. Additionally, if the server is required to enable communications to un-trusted systems, such as to serve web site content publicly, then the policy can be configured to protect all ports except for the http/https ports as required on that server.
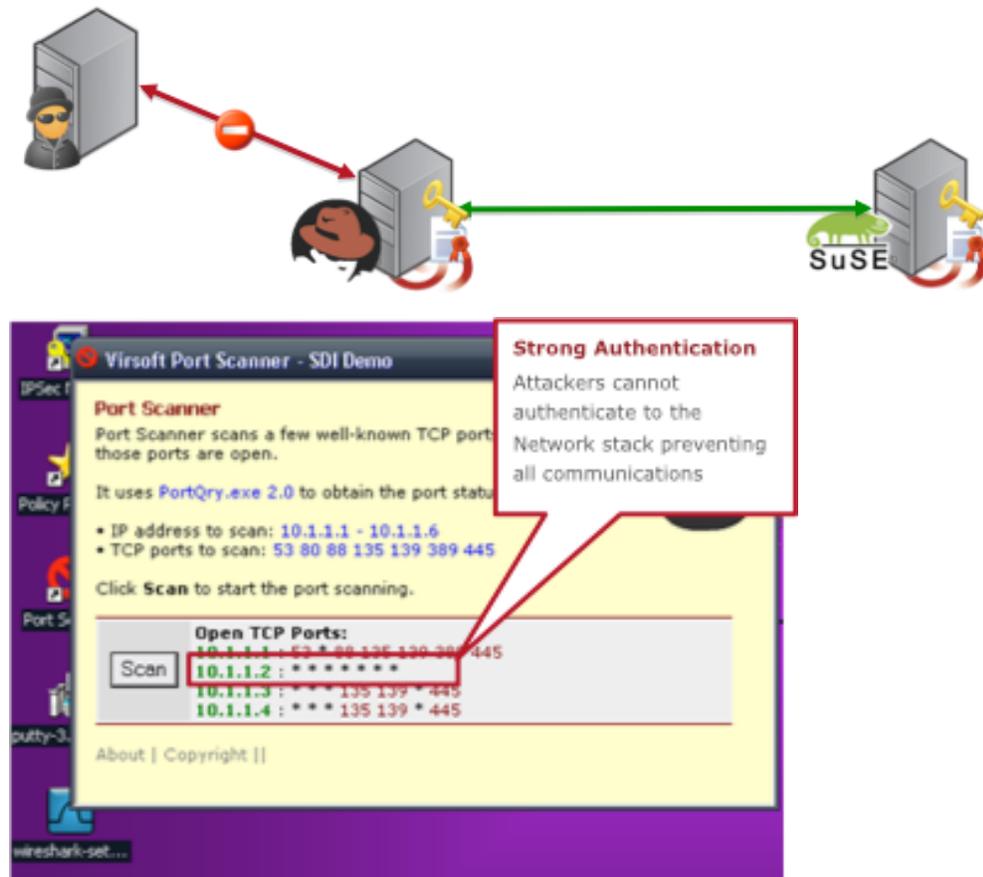
Figure 6: Server Isolation through strong authentication

The combination of these two policies enable the Enterprise to centrally define and enforce a common policy on every system that is created in the cloud, thus ensuring that the system is sufficiently protected and that they are in control of which systems can communicate to the new servers based on trusted host identities.

Establish Trusted Communications With The Enterprise

Given that there are several different Enterprise uses of Cloud Servers, there are a number of different ways for these servers to be accessed by the Enterprise. In some cases the machines will provide Internet facing services with public IP addresses which the Enterprise will use when communicating with these servers. However in other cases the servers will operate as an extension of the corporate enterprise where internal systems will need to communicate with the hosted servers but depending on the use case the hosted server may or may not need to initiate communications with other internal systems. In order to determine which communication method is best, it is important to clearly define the intended use case of the hosted server.

Cloud servers are almost always provided with private IP addresses in order to facilitate intra-cloud communications between hosted servers. This has the added benefit that the hosted server cannot be accessed from the Internet directly unless the system is either configured with an additional public IP address or specific ports from one of the hosting provider's public IP address are forwarded to the hosted system. This configuration may provide the

connectivity needed where management is performed through hosting provider specific management interfaces or directly through specific ports that are forwarded. However this limited connectivity may not provide the desired level of direct communication or management. In order to provide customers with direct management capabilities, some hosting providers will configure each cloud server with both a private IP address for intra-cloud server-to-server communications as well as a public IP address to enable external access to the new cloud server. In this scenario, it is even more important to secure the interfaces to the cloud server to ensure that access is controlled granting access only to those who really need to communicate with the server as described in the previous section. Cloud servers configured with public IP addresses can more easily support direct access by trusted enterprise systems if the communications is initiated from other Enterprise resources which may be located within the corporate network.

Several hosting providers offer an optional virtual private connectivity to enable hosted systems to communicate privately with the Enterprise. These virtual private connections are typically created by establishing a host-to-network or network-to-network VPN tunnel. These VPN tunnel connections enable hosted systems with private IP addresses to be able to communicate privately with the Enterprise network to which it is attached. While a private tunnel provide secured connectivity, it also has a few side effects which may not be desired such as the routing of all cloud server communications over the private tunnel regardless of the intended recipient of the communications. These private tunnels are network oriented vs. packet or conversation centric which forces traffic intended for an external browser to be routed through the local Enterprise network where the tunnel is terminated vs. simply being routed to the Internet through the hosting providers high bandwidth connections. Additionally, a network-to-network connections adds risk which must be accounted for in service level contracts with the hosting provider since the Enterprise will need to trust the hosting provider to not assign these private network IP addresses to any other customer's hosted systems.

The Enterprise needs a more flexible solution that enables private connectivity between cloud systems and the enterprise based on the authenticated identities of system for each packet that is communicated. This enables both the assurance that the hosted systems are only communicating with trusted systems as well as the flexibility that communications can be configured independent of the physical network infrastructure being used. This network independent secured connectivity is provided for each packet enabling traffic to be routed directly to the recipient. This means that a web server that is serving up a web site can be configured to communicate with other public browsers leveraging the hosting providers Internet connections, while simultaneously enabling secured, packet by packet, communications with other Enterprise systems for any other required traffic. This solution is provided by Centrify DirectSecure that leverages IPsec in a Transport Mode to ensure security of each individual packet between trusted systems.
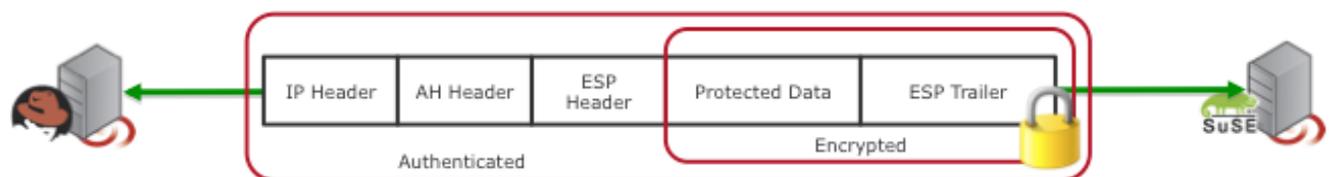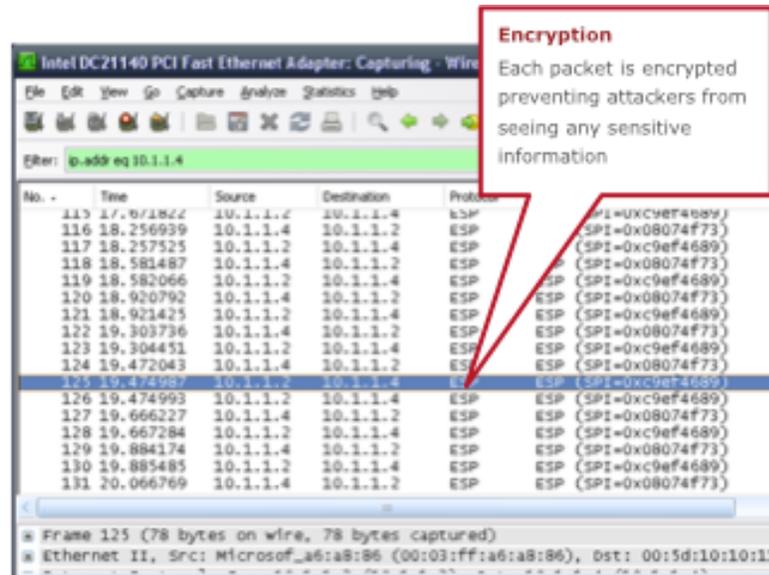
Figure 7: IPsec protected Enterprise communications

Step 4. Ensuring Visibility, Accountability and Audit on Each System

Another one of the common fears of Cloud Computing is the lack of visibility into the operation of these new servers since they are no longer located within corporate managed facilities. These new systems are typically created in a multi-tenant environment, where the servers are no longer under the watch and care of on-premise security systems where traditional IT would have visibility of all access. This new deployment model for servers increases the importance of monitoring solutions. The Enterprise looking to outsource their IT infrastructure could choose to use a hosting provider that will provide higher protection levels through dedicated or private environment. Regardless of how the hosted servers are managed, in order to protect the security integrity of the hosted environments, any administrative or privileged access to these new resources must be continuously monitored. Additionally, as organizations deploy servers in the hosted environment that may be responsible for some portion of online payment transactions, those systems must adhere to the Payment Card Industry Data Security Standard that specifically requires monitoring of all privileged access to any system.

While it is common to use a log rollup or forensic analysis tool to monitor systems, these tools can only provide reports on the activities that they were able to gather from the systems. In many cases the log information may be incomplete since the actions may not have been logged or the actions logged may not be attributed to an actual person but rather a service account. In a hosted environment it is increasingly important to ensure that Enterprise IT has appropriate user activity surveillance in place on their hosted servers in order to get the complete picture of privileged activities on these systems. User activity surveillance provides the Enterprise with a detailed account of all actions from any user who accesses their servers.

Centrify DirectAudit provides additional high definition user activity logs for each system by recording interactive user sessions. Once the user's session has been captured it is transferred to centralized storage where auditors can search across the sessions for interesting data or events and once found can replay the session to determine the

context for the actions of the privileged user. Since this solution monitors the interactive sessions of all users on the system, it provides accountability by associating all actions with the user who logged into the system, even if they switched to a service or privileged account. This points out the importance of requiring users to login with their own accounts so that regardless of what they do upon login, all actions will be recorded and properly attributed to them.
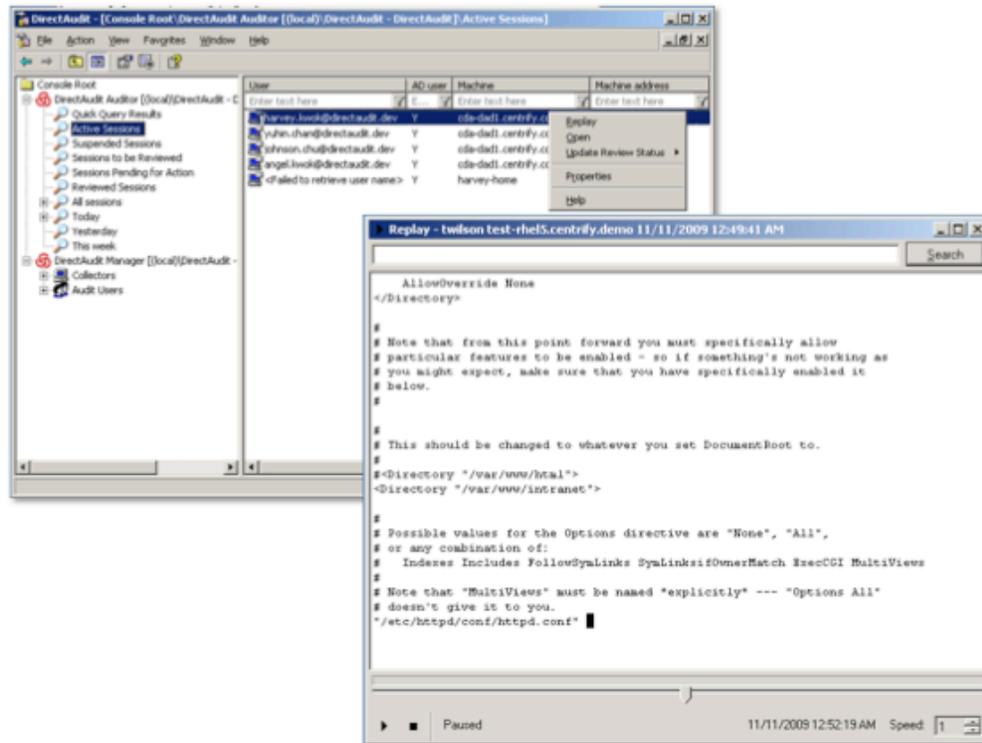

Figure 8: User activity monitoring

Step 5. Provide Enterprise-centric Single Sign-on

Cloud Servers are used for many different purposes by the Enterprise from software development to highly scalable customer facing applications. However, users will always need an account in order to log into these systems or the applications that are run on these hosted servers. Administrators and developers will need access to the operating system interfaces while end users will need access to the applications. But, regardless of who the user is that needs access, they certainly don't want to have to remember yet another userid and password to login.

Single Sign-on to the Operating Systems

Administrators who are required to manage these systems will need to log into the operating system interfaces in the hosted servers. Access to hosted Linux systems is typically through a SSH interface which can be configured to require either SSH keys, a userid and password or a Kerberos ticket. While some cloud providers have integrated ssh key issuance and management into their hosting environment's management system, these keys are typically created for the owner of the account used to manage the Enterprise's hosted environment. This keys can be provided to each administrator or developer who needs access to the hosted server, but if a policy has been

established to require individual user login to each system then each user will need their own ssh key to gain access to specific systems, thus requiring a more complex key management system. Another great feature within Active Directory is Kerberos which provides a dynamic and reusable authentication infrastructure based on a ticketing system where all users and resources share a common trust with the Active Directory Domain. This means that as long as the computer is joined to an Active Directory Domain that has a trust relationship with the Active Directory Domain where the users accounts are managed (even a one-way trust, e.g. resource domain trusts the account domain) then users will be able to seamlessly access those resources without being required to type in their userid or passwords.

Centrify Suite provides an agent for the hosted server that enables it to join Active Directory and establish the trust relationship so that Active Directory users can log into the server. In order to enable a Kerberos login to the server, Centrify also provides both a compiled version of the latest OpenSSH that has been configured to support Kerberos (for both login and key exchange) as well as a version of the popular Windows SSH client, PuTTY, that has also been enhanced to support Kerberos. This solution enables Windows users to log into their workstation with Active Directory credentials and use PuTTY to login to a hosted server running Centrify Suite with OpenSSH seamlessly. They don't need to type their userid and password since the host validation (key exchange) and user login are all validated by leveraging Active Directory identities and Kerberos tickets that were automatically issued and managed by Active Directory. This completely eliminates the need to manage SSH host keys to control access since it can be replaced by Active Directory and Centrify security policies.

Single Sign-on to the Application

Applications that run on these hosted servers provide a service to the Enterprise that in many cases will require user login. Those users may be internal employees or contractors, business partners, customers or prospects. Regardless of who the user is that needs access, they certainly don't want to have to remember yet another userid and password to login. Internal users will expect to use the application just like any other Enterprise application, accessing it seamlessly once they've logged into their desktop environment. Business partners who should be provided access will also want to gain seamless access and retain the ability to centrally control the applications that their employees are able to access. And if customers or prospects are required to login, the solution that provides authentication services should be able to support the standard userid and password based login from these users.

Just as Kerberos provides the infrastructure required to enable internal users to seamlessly login to the hosted server's operating system interfaces, Kerberos can also be used to provide Single Sign-on for applications that support the GSSAPI standard for user login functions. Some client-server applications can be configured to use GSSAPI in order to authenticate Windows users such as Sybase, Oracle with the Advanced Security Option. Centrify also provides an LDAPv3 interface to act as a proxy for LDAP enabled applications to be able to find and request information about Active Directory users without the application having to know anything more about the multi-LDAP Tree structure of a multi-Domain Active Directory infrastructure. These components of the Centrify Suite significantly simply the configuration of hosted applications in order to support Active Directory-based user login.

The more common web centric application will typically require an authentication module in order to provide single sign-on for Active Directory users. Centrify Suite provides a set of modules for each of the more popular web infrastructures from Apache Server to the J2EE app servers such as WebLogic, WebSphere, Tomcat and JBoss.

Centrify provides an agent module that provides both SPNEGO style Single Sign-on using Active Directory Keberos or NTLM-based authentication as well as Active Directory Federation Service (ADFS) based Single Sign-on which supports WS-Trust, WS-Federation and SAML. The use of ADFS solution enables Linux-based web applications with Centrify installed to support Single Sign-on for both internal users as well as business partners who have established a trust relationship. ADFS can be configured to support other external user authentication from accounts that are stored in other database or directory repositories.

Centrify Suite Overview

The combined capabilities of the Centrify Suite complement each other to enforce the following system security methodology through integration with Active Directory.

System security provided by Centrify Suite:

- The system joins Active Directory to establish a trust relationship with Active Directory as the central security policy storage

- Group Policy enforcement of Public Key Policies such as (a) Autoenrollment Settings and (b) Trusted Root Certificate Authorities establish the PKI computer credentials and trust relationships on all computers, enabling strong computer authentication.

- Group Policy enforcement of the IP Security Policies defines the IPsec policy to control how each computer will communicate on the network.

- Group Policy enforcement of "Access this computer from the network" establishes the authorized set of computers that can communicate with each other.

- Group Policy enforcement of Centrify-specific settings for Linux systems firewall settings ensures that every system will block all traffic except for the specific ports opened by this policy to further protect the system.

- DirectControl defines the identities of a set of users who both must have a valid Active Directory account as well as be a member of the Centrify Zone in order to gain access to the set of computers in that Zone.

- DirectAuthorize further defines the specific login interfaces and privileges granted to users who are assigned to specific roles in order to minimize exposure to these privileged commands and sensitive systems.

- DirectControl can then be used to lock down and manage the local accounts such as root as well as other service accounts required by specific applications such as Oracle, so that users and administrators cannot use these accounts to perform actions without being held accountable.

- DirectAudit monitors and records the activities of all users accessing these systems so that auditors and administrators can determine the root cause of problems as they arise, as well as ensure accountability and deniability for any actions performed on these systems.

The key to enabling IT to deploy a solution that provides this critical level of security for their sensitive systems is the simplified administration model based on the integration with the existing Active Directory infrastructure found in most enterprises today. This tight integration enables rapid adoption within IT as it reuses existing infrastructure and management processes that are already well known by current staff.

Summary

Centrify leverages Active Directory to enable IT to secure mission critical systems and the applications that run on them regardless of whether these systems are in your data center on traditional hardware, running as an internal cloud, hosted in your DMZ or hosted by within an Infrastructure as a Service environment such as Amazon's EC2. Centrify provides a comprehensive Enterprise security solution designed to automatically secure UNIX and Linux systems in order to enable their secured use in these environments. Leveraging both Active Directory as well as IPsec based Server and Domain Isolation technologies for both Windows and UNIX/Linux systems, enables the secured use of these resources within Cloud environments. These systems are centrally secured, user access is controlled and they are isolated on the network from any untrusted communications. The Active Directory-based security infrastructure additionally enables the Enterprise to leverage both existing IT processes such as account and security policy administration as well as to enable their existing users to access these new resources with their current Active Directory accounts. The resulting environment enables the organization to extend their computing infrastructure out to cloud based systems leveraging Active Directory to provide 5 key security controls in order to maximize the success of cloud server projects by IT organizations:

- Automate Enterprise security controls on hosted systems

- Centralize account, access and privilege management

- Isolate hosted systems hardening network access

- Ensure visibility, accountability and audit on each system

- Provide Enterprise-centric Single Sign-on

There are several ways to get started today by installing Centrify Suite on your own internal or cloud systems, start a cloud server instance with Centrify Suite pre-installed such as the Centrify Express AMIs for Amazon EC2 or use cloud servers at one of our Managed Service Providers such as Savvis and ViaWest.

Additional Reading

- Centrify White Paper "Centralized Identity and Access Management of Cross-Platform Systems and Applications with Active Directory and the Centrify Suite"

- Centrify White Paper "Top Five Benefits of Using Windows Group Policy to Secure and Manage UNIX, Linux and Mac Systems"

- Centrify White Paper "Single Sign-On and Federation for Java/Web with Centrify DirectControl and Microsoft Active Directory"

- Centrify White Paper "Protecting Sensitive Information through IPsec-Based Server and Domain Isolation"

- Microsoft White Paper "Server and Domain Isolation Using IPsec and Group Policy"
  http://go.microsoft.com/fwlink/?linkid=33947

- Microsoft White Paper "Active Directory Domain Services in the Perimeter Network (Windows Server 2008)
  http://go.microsoft.com/fwlink/?LinkId=150091

How to Contact Centrify

Worldwide Headquarters

Centrify Corporation
785 N. Mary Avenue
Suite 200
Sunnyvale, CA 94085
Phone: +1 (408) 542-7500
Email: info@centrify.com

International Locations

Centrify EMEA
Lily Hill House
Lily Hill Road
Bracknell
Berkshire RG12 2SJ
United Kingdom
Phone: +44 (0) 1344 317950

Centrify Asia Pacific
4/58 High St., Suite #105
Toowong, QLD 4066
Australia
Phone: (+61) 1300 795 789