ssh
Securing the path to your information assets

An Identity Management Application Note

Missing Identities

What Active Directory Doesn't See

Identity management in large heterogeneous IT environments is complex and in many enterprises, a work in progress. The fundamental challenge is how to bring disparate operating systems and authentication systems under central management including a unified directory where all identities reside. The benefits are significant. Centralized identity management offers better security, administrative efficiency and the end user convenience of single sign on. There are solutions that provide the glue that binds disparate systems together under a unified directory structure. However, few if any of them include access controls for identities that drive automated processes. As more and more data center and business processes are automated, the number of machine identities keeps rising even as the number of interactive user identities remains static or even declines. The result is centralized identity management governance is addressing an ever shrinking share of overall identities enterprise wide. This application note discusses the underlying difficulties in managing machine identities and describes a practical solution to this complex problem.

Machine Identities: Who Are These Guys?

Machine identities can enable process automation as illustrated in the following examples:

- System health and monitoring solutions automatically connect to multiple servers in order to collect log information.
- Automated file transfer of purchase and credit card information from point of sale devices to data center servers.
- Regular data base backups.

Secure Shell (SSH) using SSH public/private key pairs to authenticate machine based identities is widely used for process automation. In many cases there is no central directory store of machine based identities or the related authentication credentials, SSH keys.. The machine requesting access to another machine (e.g. log manager requesting access to server logs) authenticates directly via an SSH private user key, rather than having the authentication request processed by a directory such as AD. This opens a number of security and access management headaches including difficulty in tracking the identities, controlling their use and preventing identity compromise. So why don't enterprises simply move these identities and authentication processes to a centralized, AD/Kerberos based system? Unfortunately there are some significant barriers to achieving this:

1. Migrating all the Unix local user accounts into AD can be a massive effort.
2. Due to localized nature of these accounts, accounts may share the same UIDs and other conflicting information which makes the migration into individual AD accounts more complex.
3. Even if the account migration can be completed successfully, accounts often have many authorized public keys and there is often little or no information as to where the corresponding private keys reside, who owns them and what processes they support. In the absence of this information there is no way to remove and replace these authorizations in AD without causing major risk of disrupting vital business processes.
3. AD/Kerberos requires end user interaction when the first ticket is requested. There are workarounds to make this work on automated processes such as hard coding AD credentials in a startup script, Kerberos keytab or password files but these approaches raise other security concerns.
4. Some automated processes may have hard coded authentication settings, for example enforcement of defined SSH key or built-in credentials, and changing authentication to Kerberos may break those automated processes.
5. Non-Windows systems (Unix, Linux, IBM USS, MAC) do not have native support for AD authentication, so all servers need to be updated with add on PAM modules or commercial tools.
6. By default, Kerberos provides Kerberos realm wide authentication to all the defined user accounts and further access controls are configured through AD group memberships or through commercial tools. Tightening up access controls on automated identities may be problematic as grouping of application identities and their connection points is not as straightforward as human user identities.

Centralized identity management solutions such as Centrify and CA SiteMinder have robust PAM support for attaching non-Windows systems to AD environments. Unfortunately they don't address the challenge of migrating business processes. In short, there is no practical way to get from here to there.

A Structured Approach to Machine Identity Management

The challenge of unmanaged machine identities has grown over time. Data center growth has been explosive. Large server infrastructures can be home to hundreds of thousands or even millions of secure shell user key based identities. Universal SSH Key Manager (UKM) from SSH Communications Security centralizes identity information and provides a structured and non-disruptive approach for migration. The UKM approach accomplishes the following:

1. Discovers all the identities across local and centralized repositories.
2. Monitors all the identities and trust-relations, what are the connection endpoints (who is accessing where using what user accounts), determining which are not used, which are used and what processes they support.
3. Remediates – removes authorizations that are legacy or against defined access policies and makes necessary changes to authorizations in accordance with company specific policy.
4. Locks down the infrastructure – makes sure no identity moves, adds or changes occur outside of central management.
5. UKM can be deployed as a standalone solution or as part of a broader AD/Kerberos based solution that includes privileged users such as systems administrators and application developers Only UKM provides non-disruptive visibility and tools to identify and manage machine based identities which are the critical success factors for addressing this identity management challenge.

UKM is helping some of the world's largest institutions solve the problem of managing machine based identities.

For more information please visit **www.ssh.com/ukm**