Automated *NIX Identity Management Sales Play for Channel Use

Overview

Opportunity

Most orgs will have UNIX and/or Linux systems vs. being Windows only. These *NIX systems typically support apps and databases that they run either on-prem or in cloud environments. Linux has become the most used server operating system with a 68% to 31.7% lead over Windows when looking at both paid and non-paid distributions (IDC, 2018).

Introducing the Centrify Solution:

Elevator Pitch

Manually managing your *NIX estate can be time consuming, costly, and can open you up to risk. Centralizing identity management of your UNIX/Linux estate rather than using local accounts reduces costs, increases security, and eases audits due to consistent controls across *NIX and Windows.

Why Centrify Wins

- Industry recognized best solution for AD integration (sources: Gartner, Forrester, and Customer References)
- Seamless integration into AD: There's no AD Environment that we've not seen over the last 16 years. Centrify does not require ANY changes to the AD infrastructure
- Delegated Administration and Separation of Duties: Our patented, hierarchical zone-based management model enables AD admins to delegate admin control for *NIX-specific data independent of normal AD objects. That means *NIX admins can manage *NIX properties without needing management permissions on User or Group objects within AD
- Hierarchical zones enable *NIX admins to create a Zone for each group of systems that share a common *NIX namespace or where they need to delegate management of that Zone to a different group of *NIX admins
- Simplified account admin. Centrify enables admins to use AD to specify users or groups that can login to UNIX or Linux systems, centralizing all user account administration in AD. There's no need to touch *NIX systems as they all trust AD
- Service accounts for UNIX/Linux can also be managed within AD vs. created locally
- Centrify also enables centralized administration of local accounts and groups on UNIX and Linux systems where credential management can easily be integrated with a password vault
- Holistic solution: tight integration between functions of the solution.
  - » Privilege Elevation coupled with AD Authentication as defined by Roles within the Centrify Zone
  - » Session Audit coupled with both Privilege Elevation and Access Authorization, enabling admins to require session audit before granting privilege elevation rights
  - » MFA and Workflow integrated into the Centrify Platform
- Simplifies administration as well as integrating into the entire AD ecosystem.
  - » Local Account and Group management — ex. HSBC
  - » Group Policy enforcement automates security policy configuration — ex. US Gov
  - » Microsoft Certificate Authority integration for automated Server PKI Certificate issuance and renewal — just like Windows machines
  - » Application integration to AD via LDAP Proxy to simplify LDAP-aware application access to complex AD Forests with multiple Domains
  - » Kerberos keytab management automates manual tasks

Customer Benefits

- Reduce costs of identity management for *NIX by centralizing management of user accounts and groups, Sudoer rights, system configurations, and lifecycle management including provisioning and de-provisioning
- Ease of use for administrators by using their directory credentials rather than password resets or checking in and out of a password vault
- Improve your compliance posture and reduce cost of audits by having consistent controls across Windows and *NIX
- Reduce risk and increasing accountability by consolidating identities and utilizing federation rather than creating and managing local accounts or using shared accounts.

Discovery Questions (to Identify Core Needs and Pain Points)

1. **Does your environment consist of UNIX or Linux systems with complex and difficult to manage identity and group information?**

   If yes: discuss the advantages of a centralized approach either in Active Directory or Centrify platform.

   - » Do differences on individual systems make consolidation of identities difficult?
   - » Do you have different groups of systems managed by different teams?
   - » Do you have multiple AD domains that you need to integrate with? Discuss how SSSD will not suffice for complex AD environments with one-way trust

2. **How are you managing User Identity and Accounts or Groups and their memberships on your UNIX/ Linux servers today? Locally on each machine?**

   If yes: discuss the usability and security advantages of centralizing and federating access from Active Directory or the Centrify platform.

   - » Do you have a challenge with orphaned accounts on each system?
   - » Can you terminate someone and make sure that they don't have an account left behind somewhere?
   - » Are you comfortable with your company's process for provisioning and especially de-provisioning users' access to key systems?
   - » How long does it take to remove all access rights for an existing employee or contractor? How confident are you that access to all systems and applications has been disabled?

3. **How do you manage Service Accounts? What about privileges and policies? Are you managing locally on each individual machine? How much does that cost you? Do manual efforts create errors and inconsistencies that could result in compliance or security issues?**

   If yes: discuss the usability, compliance, and security advantages towards a centralized approach that is also consistent with Windows infrastructure.

4. **Are you concerned that access rights are too broad for a users' role? Can you grant rights at a granular level such as for a single system, group of systems, specific commands or grant rights for a limited timeframe?**

   If yes: least privilege can be used BOTH to prevent elevated access on an individual machine, but also to stem lateral movement across the network by granting granular rights to groups of systems. Preventing lateral movement is a CRITICAL aspect of attack chain security.

5. **To what extent do your users share passwords? Does that cause security or compliance concerns?**

   If yes: you should be concerned with this practice. How are passwords rotated? Federation and temporary tokens are always more secure than static passwords. Fundamentally shared passwords are always a bad idea.

6. **Do you have applications running on your *NIX systems that require authentication for AD users?**

   If yes: how are you achieving that today? It can easily be done via Kerberos and all management centralized in Active Directory.

   - » Do these apps use LDAP to talk with AD today? Are they limited to one Domain?
   - » Do these apps have other computers as clients where they are sharing a static password? Security will be better and simpler via Kerberos

7. **Are you using NIS (Network Information Service) or LDAP for managing *Nix devices?**

   If yes: discuss the advantages of using Active Directory or Centrify platform for management.

   - » Do you have security and compliance concerns about your legacy NIS and netgroups infrastructure?
   - » Do you have NAS systems that require the same *NIX identity information as your systems?
   - » Does your environment require separation of duties and delegated administration?