Volume : 1 | Issue : 7 | Dec 2012 • ISSN No 2277 - 8179

Research Paper

Server Access Control

Engineering

KEYWORDS : Access control, servers, authentication, and authorization and polices

Anitha Chepuru	Associate Professor IT Dept, G.Narayanamma Institute of Technology and Science (for women), Shaikpet, Hyderabad - 500008, Andhra Pradesh, India
Dr.K.Venugopal Rao	Professor CSE Dept, G.Narayanamma Institute of Technology and Science (for women), Shaikpet, Hyderabad - 500008, Andhra Pradesh, India
Amardeep Matta	Application Security Solution Consultant, Identity and Access Management –Practice, Mahindra Satyam Computer Service Ltd, Hyderabad, Andhra Pradesh, India

ABSTRACT

This paper describes the concepts centralized security policies by which we can provide a total security solution for open native operating systems. Today every organization requires high level protection against external threats and internal user activities. Organizations face a number of critical requirements for access control for their resources. All organizations are under increasing pressure to be more competitive and compliant. As key business enabler, must protect all their critical applications. As all critical applications and sensitive data reside with Operating System, effective management and enforcement of OS access is of paramount importance. Disclosure rules should be implemented and enforced consistently across to help protect data. This can be particularly challenging as today's organizations infrastructure invariably support a number of heterogeneous operating systems. For authentication and user management, UNIX / Linux systems provide native local account management capability which again very costly to administer. While another method Network information service (NIS) provides a centralized approach for authentication but it has its own significant security issues. This Server Access Control (SAC) for operating system solution provides centralized authentication, password management, high scalability, availability, security and account management for critical servers..This access control solution will help organization securely manage access to business critical servers / operating systems by giving users proper access they need.

- *Defends against the top security threat that enterprises face: malicious or fraudulent behavior by internal users and employees*
- *Combines full-fledged intrusion prevention-host-based firewall, application and platform protection, user tracking and controls-with robust auditing and compliance checking*
- *Provides Persistent Universal Auditing to document compliance with government regulations, corporate policy and other security mandates*
- *Provides best-practice security policy templates to minimize implementation effort and time*
- *Delivers mainframe-class security and auditing in a lightweight, easy-to-use.*

Introduction:

Most organizations have a variety of server platforms with different security capabilities and interfaces. Trying to manage security policies and track access rights in this type of environment is a time-consuming and expensive process, as traditional operating system security is not built to handle this type of scenario. Many systems have just a few roles or an all-or nothing approach that revolves around a super user accounts. If users need any kind of privileged access, they are often given the right to one of these shared super user accounts, affording the user unlimited rights and anonymous access to the server. Worse still, the method by which these accounts are shared is through a single account password, which increases the risk of this password being exposed outside of the intended team. Over time, more and more people gain access this way and the risk to the organization multiplies because of the overexposure to sensitive resources.

The type of adversary we face is evolving, as it is no longer valid to assume attackers are "out there" as nameless, faceless hackers. Today, the attacker is just as likely to be a disgruntled employee, saboteur, business partner with questionable ethics and loyalties. Thus, you need to protect your server resources from both the external attacker (who are still out there) and internal personnel — especially super users, whom have access to all the sensitive data residing on every server they can access. The complexity of protecting servers and ensuring accountability amongst these super users is significant. A common technique used by server administrators is to share super user accounts and use generic logins like "administrator" or "root." These shared accounts don't provide the necessary segregation of duties, provide no accountability for individual actions and even have the ability to turn off event logs. This has led to the many of the publicized data breaches and security problems that have been in the news.

DATA ACCESS these shared accounts typically result in providing over-privileged users with access to critical systems and data, predominately because it's too hard to manage a policy across thousands of servers with granular access rules. The combination of over privileged access with administrator carelessness can often impact business continuity. Meanwhile, the lack of accountability makes it almost impossible to trace back to the specific administrator who committed the errors, resulting in both security and accountability issues.

AUDIT ISSUES sharing user accounts prevents audit logs from really identifying which administrator made which changes on the servers, undermining the accountability that is so critical to meeting regulatory requirements.

Distributed data center provide a great deal of flexibility, but they also increase the need for protection from external and internal threats. The number of servers, physical and virtual, is still on the rise and the amount of critical resources that they control is increasing as well. Data center requires extensive visibility across an ever-expanding set of server resources, while ensuring accountability of changes and protecting the sensitive data that resides there. Failure to manage server resources has been directly responsible for high profile data breaches. This scenario, combined with the further specialization within IT departments, means that more people need some form of access to these machines to keep the business running smoothly. Maintaining data integrity is one of the most important jobs of the IT professional. It is a critical mistake to embrace all of these new data center scalability and flexibility technologies without weighing the security and data protection requirements related to these new technologies.

In any data center sophisticated server resource protection must be implemented to ensure these requirements are met. You are also required to provide granular audit records and reports to substantiate controls, policy status and server access logs for each audit. These regulations require fine-grained controls and cross-platform consistency to ensure the separation of

Volume : 1 | Issue : 7 | Dec 2012 • ISSN No 2277 - 8179

duties, especially in mixed operating system environments. Additionally, in the event of a compromise, the ability to research the incident forensically is also required.

As a result organizations need a central, independent security system to protect server resources across the extended enterprise, providing a flexible and accountable means to contain super user accounts by delegating necessary privileges to authorized administrators. Access Control operates at the system level to ensure efficient and consistent enforcement across all systems — including Windows, UNIX, Linux and Virtualized environments. By distributing server security policies to endpoint devices via an advanced policy management capability, can support large, global enterprise deployments. Moreover, can securely support auditing of each policy change and enforcement action in order to comply with global regulations.

Solution:
Server Access Control (SAC) provides you with a powerful solution for managing security for your native platforms, making it possible to implement a security policy that can be customized entirely to an enterprise's security requirements. SAC lets you provide security for users, groups, and resources beyond what is available in native operating systems. It lets you centrally manage security across the organization and integrate your security policies in a heterogeneous environment.

An administrator defines additional authorization policy by applying fine-grained access controls that restrict or permit access to key system resources. Controls are based on user identity, group membership, the type of operation, the time of day or the day of the week, and the accessing application. An administrator can control access to specific file resources, login and network services, and changes of identity. These controls can also be used to manage the execution of administrative procedures and to limit administrative capabilities on a per-user basis.

- Who has access to this applications and databases?
- What data - both structured and unstructured – resides in flies, databases or data stores?
- Who actually needs access to that data?
- What access control to be established as a result?

The authorization services allow an organization to securely control user access to protected information and resources. By providing a centralized, flexible, and scalable access control solution, allows highly secure and well-managed operating systems infrastructures to be built. In addition to its state-of-the-art security policy management feature, supports authentication decision enforcement for administrative users, the application of login and password policies to user accounts of underlying resources, authorization, data security, secure communication and resource management capabilities. At its core, the SAC provides role based access control: This authorization service, accessed through a standard authorization API, provides permit and deny decisions on access requests from native resource managers and third-party applications. It is the resource manager/authorization evaluator responsible for managing and protecting operating systems information and resources – it applies a centrally managed authorization and authentication policy to operating system resources.

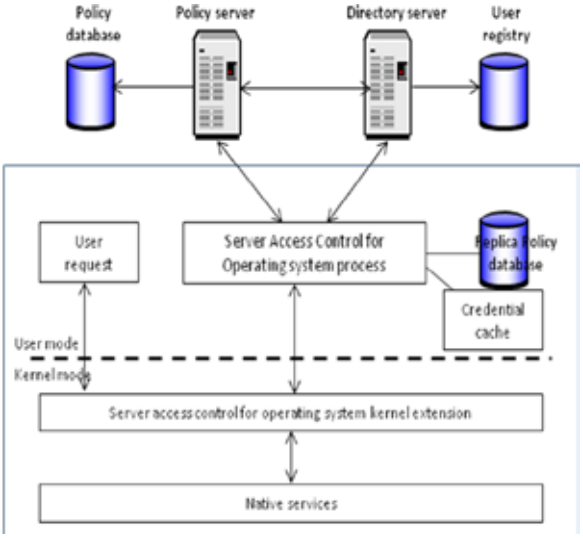
Effective host SAC management provides the ability to contain these privileged accounts by delegating necessary privileges to the appropriate personnel only when they need them. The administrators can do their jobs without exposing sensitive data or business critical resources. Additionally, such an approach ensures that there is an audit trail and enforcement of accountability over administrators and their actions.

The core elements of SAC are the secure, hardened agents that integrate natively with the operating system to enforce and audit the granular policies required to meet compliance mandates. Endpoint agents are available for all the major operating systems, including all leading Linux, UNIX and Windows versions. SAC provides a user friendly and consistent Web-based interface to manage the endpoint policies and devices. Access Control natively supports the leading virtualization platforms, including VMware ESX, Solaris and Citrix Server ensuring the hypervisor layer and the guest operating systems that run on them are protected.

In enterprise environments, using a directory for user management and directory-enabled application deployment has become common practice. SAC supports enterprise user stores; that is, stores for users and groups that are native to the OS. This native integration allows you to define access rules for your enterprise users and groups without having to synchronize or import the users and groups into the Access Control database.

Work flow:
SAC for Operating Systems is invoked immediately after the UNIX- or Linux-based operating system has completed its initialization and places hooks in system services that must be protected. These hooks pass control to SAC for operating systems before the service being requested is performed.

- When a user requests a system service for an object / server that is being protected
- SAC for Operating Systems accesses the policy information associated with the object to determine whether the user is permitted to perform the requested operation.
- The decision to allow or deny access is based on the access rules and policies that are defined in the SAC policy database by the system administrator.
- After the decision is made, the decision is logged so that the activity can be audited and appropriate corrective actions can be taken, if necessary.



Conclusion
Access Control solution provides a superior level of server resource protection and eases the administrative burden of managing security across diverse systems distributed throughout a global enterprise. No longer need to define and manage access permissions user-by-user and server-by-server. With advanced policy management, logical host grouping, and a centralized point-and-click interface to deploy corporate policies (and auditors) can be confident each user only has the rights to the data and systems necessary for his or her job function. Can enforce consistent security policies across diverse server environments by enabling user accounts, passwords and security policies to be shared across all managed servers. Location also becomes a non-issue by controlling cross-network access management from a single Web-based administrative console using advanced policy management architecture to distribute the policies to all of endpoints. Achieve unmatched flexibility by empowering administrators to specify protection at the individual system level, whole infrastructure

REFERENCE
[1] www.ca.com | [2] www.oracle.com | [3] www.ibm.com | [4] www.sun.com