Windows Least Privilege Management and Beyond

Abstract

Devising an enterprise-wide privilege access scheme for Windows systems is complex (for example, each Window system object has its own access control list and the myriad of OS level rights and integrity levels vary by Windows version). For Windows environments it is critical that organizations can delegate administration and establish granular privileges quickly and efficiently to restrict administrators so they only access the servers and resources required to perform their job and only during the approved times to perform specific tasks. Given the limitation of native tools, it has been common practice in Windows environments to assign privileged users high levels of administrative privilege so that IT staff could fix any problem that might occur at any time, even if that grants access to resources in the environment that administrators should not have privileged access to. And the requirement to meet compliance demands, mitigate insider risk and manage access and privileges of temporary workers, contractors and third-parties is driving the requirement for least-privilege security across the Windows environment and beyond to UNIX and Linux systems regardless of where these systems run – on-premise or in the cloud. Centrify DirectAuthorize for Windows eliminates the problem of too many users having broad and unmanaged administrative powers by delivering secure delegation of privileged access and granularly enforcing who can perform what administrative functions. An integrated component of the Centrify Suite, organizations can easily extend DirectAuthorize to UNIX and Linux systems and enable user level auditing across Windows and non-Windows systems. The result is organizations can more easily meet compliance requirements and improve security.
Introduction

Devising an enterprise-wide privilege access scheme for Windows systems is complex (for example, each Window system object has its own access control list and the myriad of OS level rights and integrity levels vary by Windows version). This complexity is increased with hybridization of the data center environment that includes a mix of physical and virtual systems deployed on-premise and in cloud environments. And even organizations that heavily invest in Windows servers are increasingly likely to have a mix of Windows, UNIX and Linux systems as they take advantage of cloud environments. Establishing and maintaining a security and compliance posture, in this dynamically changing environment, is regularly cited as the top concern of IT leaders who are responsible for mitigating risk and protecting the information assets of their enterprises.

For Windows environments it is critical that organizations can delegate administration and establish granular privileges quickly and efficiently to restrict administrators so they only access the servers and resources required to perform their job and only during the approved times to perform specific tasks. This is even more critical as IT organizations make use of temporary workers and contractors and increasingly rely on third-party service providers to manage critical parts of their information systems. How do diligent IT leaders implement a least-privilege security model in this complex environment to guard against the misuse and abuse of overly broad administrative privileges in Windows environments and across their evolving data center?

Native Windows Capabilities Fail to Address Requirements

In Windows environments there are many types of users who have privileged administrative access to servers. For example, there are Domain Administrators who manage Active Directory services and Domain Controllers, System Administrators who install and configure the Windows systems, and Application Administrators who manage the various specialized Windows Servers such as Exchange, SQL Server and IIS Web servers.

Given the limitation of native tools it has been common practice in Windows environments to assign privileged users high levels of administrative privilege so that IT staff could fix any problem that might occur at any time, even if that grants access to resources in the environment that administrators should not have privileged access to. Unfortunately, many security experts and auditors have identified too many privileges as a primary focus for improved security and compliance. Least-privilege access is now a top priority for IT organizations. In fact, Gartner’s Hype Cycle for Identity and Access Management Technologies, 2012 report recommends a granular least-privilege model:

"Adopt a ‘least privilege’ model for granting privileges, including superuser privileges. It is not good practice for administrators to use a privileged account for mundane activities… there is a need for the organization to have more granular control over and visibility into the way that these [administrator] privileges are granted and used."

Some organizations might think the native capabilities using Windows groups can support a least-privilege security model. Unfortunately, even in recent Windows versions built-in groups do not allow organizations to grant access to only the privileges needed for users to perform their job, restricted to specific resources and for limited time periods. And group polices just don’t scale as the number of administrator roles and servers increase.
Least Privilege Addresses Critical Challenges

Compliance Demands

The myriad of compliance regulations create ongoing challenges for enterprises in every industry, and many companies must meet multiple requirements for internal controls (SOX), security of payments data (PCI DSS), patient health information (HIPAA) and other industry-specific requirements (GBLA, NERC and FISMA/NIST SP 800-53). Common to every major compliance regulation and industry mandate are requirements to ensure users authenticate with a unique identity (and not share accounts) and privileges are limited to only ones needed to perform job functions. In addition, user activity must be tracked and monitored with enough detail to determine the effectiveness of the security controls the organization has put in place.

All major compliance standards require least-privilege security.

Sample of major least-privilege security compliance requirements

<table>
<thead>
<tr>
<th>Compliance rule</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SOX</strong></td>
<td>Section 404</td>
</tr>
<tr>
<td></td>
<td>Requires security controls that ensure only authorized users have access to enterprise IT resources and financial information. Section 404 also requires that security controls be demonstrably effective.</td>
</tr>
<tr>
<td><strong>GBLA</strong></td>
<td>Section 501 (b) and FTC Safeguards Rule</td>
</tr>
<tr>
<td></td>
<td>This rule requires financial institutions to have an information security plan that “contains administrative, technical, and physical safeguards” to “insure the security and confidentiality of customer information: protect against any anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.”</td>
</tr>
<tr>
<td><strong>PCI DSS</strong></td>
<td>Requirement 7: Restrict access to cardholder data by business need to know</td>
</tr>
<tr>
<td></td>
<td>- 7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following:</td>
</tr>
<tr>
<td></td>
<td>o Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities</td>
</tr>
<tr>
<td></td>
<td>o Assignment of privileges is based on individual personnel’s job classification and function</td>
</tr>
<tr>
<td></td>
<td>o Implementation of an automated access control system</td>
</tr>
<tr>
<td></td>
<td>- 7.2 Establish an access control system for systems components with multiple users that restricts access based on a user’s need to know, and is set to “deny all” unless specifically allowed.</td>
</tr>
<tr>
<td>Compliance rule</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| **HIPAA**       | HIPAA Technical Safeguards (§164.312)  
Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights. |
| **FISMA/NIST SP 800-53** | AC-3 Access Enforcement  
- The information system enforces approved authorization for logical access to the system in accordance with applicable policy.  
AC-5 Separation of Duties  
- Separate duties of individuals as necessary, to prevent malevolent activity without collusion and implement separation of duties through assigned information system access authorizations.  
AC-6 Least Privilege  
- The organization employs the concept of least privilege, allowing only authorized access for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational mission and business functions. |
| **NERC**        | CIP 007-3 R5  
The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of “need to know” with respect to work functions performed. |

Compliance specifications often refer to “need-to-know” or “business need-to-know” when describing a specific authorization control. In order to fully address these compliance rules and satisfy internal and external auditors, organizations should also track and monitor privileged activity. Tracking privileged activity including elevated privileges is a critical part of fully meeting least-privilege compliance requirements.

**Mitigating Insider Attacks**

Mitigating the risk of insider attacks that can lead to a data breach or system outage remains a key concern for IT security managers. Several factors have led to an increase in insider incidents including the sharing of privileged account credentials and assignment of privileges that are overly broad with respect to the job responsibilities of the user.

**Temporary Workers, Contractors and Third-Party Access**

Today’s business environment is driving enterprises to find cost efficiencies at every level of their operations. Temporary workers, contractors and cloud computing are giving organizations the agility, flexibility and cost controls they require to remain competitive, but organizations are still responsible for
the security and compliance of their IT systems. This is made clear in compliance requirements that specifically call out responsibilities when leveraging third-party service providers and outsourcing firms.

Third-party user access creates even more impetus to implement least-privilege security. In addition to the insider attacks and compliance demands already mentioned, third-party access increases the pressure to limit privileges on target resources and to restrict timeframes for third-party access.

**Key Capabilities to Consider**

Most privilege management vendors provide single-purpose products that don’t provide integrated, unified identity and privilege management across cross-platform systems in the data center. Additionally, most solutions can’t offer a single architecture to support systems on-premise in the data center and those “outside the firewall” in the cloud. Finally, many Windows privilege elevation products only elevate privileges locally by giving the user local Administrator privileges.

When deploying single-purpose Windows Privilege Management, key capabilities that should be considered are:

- Easy user interface for privilege elevation that does not require passwords to be re-entered or users to even know administrative passwords
- Restrict privileges by time, specific system or service/application
- Integrated user-session auditing that includes capture, search and playback of session video, metadata and events
- Trigger user-session auditing based on specific user, role, system or elevation
- Single integrated architecture for delegation and privilege management across Windows, UNIX and Linux with roles and rights centrally stored in Active Directory
- One console to manage user privilege and roles across Windows, UNIX and Linux

**Centrify DirectAuthorize Solution**

Centrify DirectAuthorize for Windows eliminates the problem of too many users having broad and unmanaged administrative powers by delivering secure delegation of privileged access and granularly enforcing who can perform what administrative functions. An integrated component of the Centrify Suite, organizations can easily also extend DirectAuthorize to UNIX and Linux systems and enable user level auditing across Windows and non-Windows systems. The result is organizations can more easily meet compliance requirements and improve security.

**How Centrify DirectAuthorize for Windows Works**

DirectAuthorize for Windows — an integrated component of the Centrify Suite — lets IT organizations securely delegate and manage privileged access across your entire Windows infrastructure. DirectAuthorize also delivers seamless integration with Centrify DirectAudit to enable IT to achieve stronger security and governance by enforcing least-privilege access and detailed monitoring of privileged user sessions.
DirectAuthorize for Windows is comprised of three main components that install quickly and easily with guided wizards for deployment.

These components are:

- **Centrify DirectManage Console** — a Windows-based console to configure roles with specific roles and rights. Roles grant privileged users limited capabilities over a subset of resources. This enables least-privilege access to systems, services and applications that make up your Windows environments. These roles and rights are then assigned to Active Directory users and groups, making the management of granular access simple and straightforward.

- **Centrify DirectAuthorize Agent** — a Windows service that enforces privileged access to systems, services and applications using the roles and rights defined in the Centrify DirectManage Console and centrally stored in Active Directory. The DirectAuthorize Agent works with the server’s authentication and access management processes to examine all of the actions performed by users on a system. The DirectAuthorize Agent also includes a command-line option to enable privilege elevation within PowerShell or VB scripts. In addition, the DirectAuthorize Agent can trigger auditing of user-sessions by user, role, system or privilege elevation. This audit trail feature sends requests to the Centrify DirectAudit Agent, which starts and stops session recording for defined actions by capturing session events, metadata and optionally video for search and playback. The Centrify DirectAudit Agent is easily installed alongside the DirectAuthorize Agent.

- **Centrify Elevation Tool** — a Windows tool available in the desktop system tray of every system that you install the DirectAuthorize Agent on. The Elevation Tool provides a fast, one-click interface to elevate privilege to specific roles enabled through the Centrify DirectManage Console and enforced on the local server by the DirectAuthorize Agent. The Elevation Tool supports customized settings for one-touch keyboard shortcuts, making switching between multiple privileged desktops quick and easy.
Centrify DirectAuthorize for Windows lets users elevate privilege using a one-click Centrify Tray Application to create a new desktop for an assigned administrative role or use 'Run as Role' for privilege elevation for a single application.

The operation of DirectAuthorize begins with defining roles and rights using the DirectManage Console, with the end goal being to set up a least-privilege environment so that users only have specific privileges to perform their jobs and revert to normal user access during other times and always authenticate with their unique Active Directory credential. You can also turn on auditing to verify users are not misusing privileges granted to them.

For example, you can define a role called “SQL Developer” that can create and modify SQL Server-based applications, but cannot start, stop or reset the server — a different role called “SQL Server Admin” grants those privileges. Another role can be defined for management of an Active Directory group of Exchange Server administrators for the company’s Exchange Servers, but only a subset of the Exchange administrators are permitted to configure the Exchange Servers of the company that was just acquired. Centrify even enforces who can elevate privilege into a Windows system across the network, which is not possible with native Windows tools.

Once roles are defined, they are assigned to Active Directory users and groups. For example, you may assign Jane the “SQL Developer” role and the “SQL Server Admin” role. Provisioning is easy — just associate each role with the relevant Active Directory groups.

DirectAuthorize for Windows also supports time-limiting of roles. You can easily configure time limits by hour of the day or day of the week in order to improve control and visibility of temporary workers, contractors, partners and offshore staff who require access to your company’s important IT assets. Time limiting is just one of the powerful features in DirectAuthorize for Windows that is hard to achieve with Windows native controls. Another example is DirectAuthorize’s Zones capability. You can use Zones to define delegated administration for specific users and computers, assign roles and rights and link audit triggers to users, roles, servers and privilege elevation. Zones can also be used to create consistent access and privilege management across platforms, applications and databases. For example, a “Database Admin” Zone can include not only Oracle Administrators responsible for databases running on Solaris but also SQL Server Administrators using Windows systems — common access rules and privileges are defined and managed centrally.

Once roles and rights are defined and assigned to Active Directory users and groups, the DirectAuthorize Agent enforces these roles and rights on the managed systems. If a user is granted multiple roles on a given system or application, they can use the DirectAuthorize Elevation Tool to quickly and easily switch...
roles. DirectAuthorize’s one-click privilege elevation and privilege desktop switching improves user productivity by eliminating the need to re-enter passwords, check out temporary passwords or submit help desk requests for access while maintaining least-access security.

Finally, you can also use DirectAuthorize to enable session auditing and replay via DirectAuthorize’s seamless integration with DirectAudit. With DirectAudit, detailed sessions and events can be captured whenever users elevate privilege, access high-value IT assets or perform day-to-day tasks that require tracking for compliance and corporate governance. Triggering DirectAudit only requires adding auditing as a property to any user, role, system or privilege. This is supplemented by DirectAuthorize’s own audit-logging capability, which sends privileged user events to the Windows event log. Native Windows management tools do not have user-session capture and replay to monitor user actions and therefore do not meet stringent compliance requirements.

Centrify DirectAuthorize Benefits

Centrify DirectAuthorize helps an organization quickly achieve least-privilege access to Windows systems, allowing them to gain control and visibility over their extended data center operations and provides the following business benefits:

- Strengthen Security and Reduce Operational Risk. DirectAuthorize for Windows strengthens security through delegated administration, separation of duties and granular access control so organizations can enforce least-access privileges, thereby reducing the risk of unauthorized access to Windows systems, applications and services.

- Dramatically Improve Compliance. DirectAuthorize for Windows improves compliance by providing a single, unified identity services architecture to enforce security across Windows, UNIX and Linux systems and applications while also enabling enterprise-wide user-session auditing and reporting.

- Reduce Costs and Increase Productivity. DirectAuthorize for Windows is part of single integrated solution for unified identity and privilege management across the data center, cloud and mobile, resulting in reduced costs and increased productivity when compared to deploying a myriad of single-purpose and platform-specific products.
Conclusion

Centrify DirectAuthorize for Windows addresses the “too much privilege” problem by delegating administration and limiting what administrators can do to the tasks and resources required for their job roles, while enabling a fast, simple method of privilege elevation when required. A wide range of roles and rights are available in DirectAuthorize to implement least-privilege access for any user in the environment while flexible and granular secure delegation using Centrify Zones allows for simplified management of roles and rights.

Additional Resources

Unified Identity Services White Paper – A Practical Path to Unified Identity

Privileged User Activity Auditing: The Missing Link for Enterprise Compliance and Security
http://info.centrify.com/privileged-user-activity-auditing-white-paper.html

DirectAuthorize for Windows Data Sheet

About Centrify

Centrify provides Unified Identity Services across the data center, cloud and mobile that results in one single login for users and one unified identity infrastructure for IT. Centrify’s solutions reduce costs and increase agility and security by leveraging an organization’s existing identity infrastructure to enable centralized authentication, access control, privilege management, policy enforcement and compliance. Centrify customers typically reduce their costs associated with identity lifecycle management and compliance by more than 50 percent. With more than 4,500 customers worldwide, including 40 percent of the Fortune 50 and more than 60 Federal agencies, Centrify is deployed on more than one million server, application and mobile device resources on-premise and in the cloud.