

Secure Access Control Using CentrifyDC in Heterogeneous Networks

Olena Shevchenko, Dmytro Bondarenko, Iryna Kovalenko, Andriy Melnyk
Taras Shevchenko National University of Kyiv, Ukraine

Abstract- Modern IT environments increasingly span a mix of Linux, UNIX (Solaris and AIX), and Windows systems, creating significant challenges in managing decentralized user accounts, enforcing strong authentication, and maintaining comprehensive audit trails. Security and compliance frameworks including HIPAA, SOX, and NIST SP 800-53 demand centralized control over identity and privileged access, yet many organizations still rely on fragile local account systems or disparate tools. This fragmented model often leads to inconsistent enforcement, audit gaps, and elevated risk of unauthorized access. This review examines CentrifyDC, an Active Directory bridge that delivers unified, centralized authentication and role-based access control across heterogeneous environments. By integrating with Linux Pluggable Authentication Modules (PAM), Name Service Switch (NSS), SSH, and native Role-Based Access Control (RBAC) for Solaris and AIX, CentrifyDC enables seamless AD-based login, command-level delegation, and multi-factor authentication. Privileged sessions are audited, logged, and stored centrally, bolstering compliance while minimizing reliance on sudo or multiple account stores. Deployment considerations and operational benefits are highlighted through real-world use cases from high-performance research clusters and Solaris-based healthcare infrastructure to AIX servers in government environments. CentrifyDC demonstrates how centralized policy inheritance, zone-based delegation, and secure PAM routines enforce least privilege and simplify administration across large fleets. Performance optimizations including login caching and load balancing are evaluated to ensure scalability. The review concludes with an exploration of future enhancements, such as integration with Azure Active Directory and Okta, AI-driven access risk modeling, and Infrastructure-as-Code pipelines for automated policy deployment. These developments promise to extend centralized access control into hybrid cloud environments and DevSecOps workflows. Ultimately, CentrifyDC offers a robust, compliant, and future-ready solution for managing identity and privileged access across diverse operating systems under a unified directory infrastructure.

Index Terms- CentrifyDC, Access Control, Active Directory Bridging, Privileged Access Management, UNIX Authentication, PAM Integration, Compliance Enforcement, Role-Based Access Control, Secure Login, Multi-Platform Identity Management, Linux Security, Solaris AD Integration

I. INTRODUCTION

1. Background on Multi-Platform Identity Management

In modern enterprise environments, IT infrastructures often encompass a wide range of systems, including Linux, Solaris, AIX, and Windows. Managing authentication and access control across such a heterogeneous landscape poses significant operational and security challenges. Traditional methods involve maintaining separate local user accounts and sudo configurations on each system, which quickly becomes error-prone, hard to scale, and difficult to audit. Without centralized policy control, these disparate systems leave organizations vulnerable to privilege escalation, identity theft, and non-compliance with regulatory mandates.

2. Importance of Centralized Access Governance

Centralized access control especially when linked to corporate identity sources like Active Directory (AD) is crucial to enforce consistent authentication and authorization across diverse environments. It ensures that user provisioning, access revocation, and role delegation follow a standardized and auditable workflow. Additionally, it reduces administrative burden, minimizes risk, and supports compliance with standards such as HIPAA, SOX, and PCI-DSS, which mandate tight control over privileged access and system-level changes.

3. Overview of CentrifyDC

CentrifyDC (now part of Delinea) offers a unified identity management and access control solution that bridges non-

Windows systems to Active Directory. It enables centralized authentication, fine-grained authorization, session auditing, and multi-factor authentication across Linux, UNIX, and macOS endpoints. With features like zone-based delegation, CentrifyDC aligns closely with the principles of least privilege and Zero Trust security, making it a strategic choice for hybrid and multi-platform enterprises seeking robust access governance.

II. ARCHITECTURAL FRAMEWORK OF CENTRIFYDC

1. Active Directory Bridging Model

CentrifyDC functions as a bridge between UNIX/Linux systems and Microsoft Active Directory. It allows non-Windows systems to act as AD clients, enabling users to log in with their AD credentials. The architecture uses CentrifyDC agents installed on endpoints, which interact with the AD domain controllers using Kerberos and LDAP protocols. This eliminates the need to manage local accounts and synchronizes identity enforcement across the enterprise.

2. Key Architectural Components

The architecture includes:

- CentrifyDC Agent: Installed on UNIX/Linux endpoints to manage AD authentication and authorization.
- Zones: Logical groupings that allow hierarchical delegation of access policies.
- Group Policy Integration: AD Group Policy Objects (GPOs) can be used to enforce security settings on UNIX/Linux systems.
- Centrify DirectAudit: Captures and replays user sessions for forensic analysis and compliance.

CentrifyDC is designed to scale across thousands of systems using multi-threaded architecture, caching mechanisms for offline authentication, and support for geographically distributed AD environments.

3. Interoperability with Native OS Tools

CentrifyDC leverages native OS mechanisms such as Pluggable Authentication Modules (PAM), Name Service Switch (NSS), and Role-Based Access Control (RBAC). On Solaris, it integrates with SMF services and RBAC profiles, while on Linux it modifies PAM stacks and sudoers policies. This native compatibility ensures low operational disruption and facilitates tight integration with existing security controls and system behaviors.

III. KEY FEATURES AND CAPABILITIES

1. Centralized Authentication and Single Sign-On (SSO)

One of CentrifyDC's core strengths is enabling centralized login using AD credentials across all supported platforms.

This SSO capability reduces password fatigue, strengthens password policies, and improves user experience while simplifying account management. By binding UNIX/Linux systems to AD, organizations eliminate local account drift and maintain consistent authentication logic.

2. Role-Based Access Control (RBAC)

CentrifyDC enables fine-grained RBAC across heterogeneous systems through its zone model. Zones allow administrators to define user roles, permissible commands, time-of-day access, and host restrictions all centrally. For Solaris and AIX, it integrates with the OS-native RBAC models, enabling privilege delegation that aligns with least-privilege principles and audit requirements.

3. Session Logging and Command Auditing

With Centrify's DirectAudit module, all privileged sessions can be recorded, indexed, and replayed. This supports detailed forensic analysis, tracks privileged command execution, and ensures accountability during security audits. Audit logs are centrally stored and protected from tampering, meeting compliance mandates such as HIPAA and FISMA.

4. Multi-Factor Authentication (MFA)

CentrifyDC supports MFA through smartcards, TOTP tokens, push-based authentication, and biometric integration. MFA can be enforced globally, per user, or based on system sensitivity, helping prevent unauthorized access even in case of compromised credentials.

IV. DEPLOYMENT CONSIDERATIONS IN MIXED UNIX ENVIRONMENTS

1. Installation and configuration for Linux, Solaris, and AIX

Deploying CentrifyDC in a heterogeneous UNIX environment requires careful attention to OS-specific nuances. On Linux platforms such as Red Hat or Ubuntu, the Centrify DirectControl agent can be installed via standard RPM or DEB packages and configured to join Active Directory with minimal system disruption. Solaris deployments often involve integrating Centrify services with the Service Management Facility (SMF) and configuring RBAC for privilege enforcement. AIX systems demand special considerations due to unique subsystems such as ODM and NIM. Across all platforms, joining the appropriate Centrify zone ensures policy inheritance and centralized control, enabling consistent identity enforcement and access governance.

2. Zone-based access segmentation

Zones in CentrifyDC enable organizations to group systems logically and define granular access rules per segment. These zones allow administrators to assign specific Active Directory users or groups to roles within designated UNIX

environments. For instance, a biomedical research team may be granted access only to Solaris servers in the sequencing cluster, while finance personnel can access AIX hosts running payroll systems. This segmentation enhances security by minimizing lateral movement and enforces the principle of least privilege across the environment.

3. Pre-deployment dependencies and environmental checks

Before initiating deployment, essential network services such as DNS and NTP must be correctly configured to ensure secure and synchronized communication with domain controllers. Kerberos authentication, a core part of CentrifyDC's architecture, depends heavily on accurate timekeeping. Firewalls must allow necessary ports for LDAP, Kerberos, and Centrify services. Pre-deployment tools offered by Centrify can validate these prerequisites, identify incompatible system configurations, and ensure that all packages and libraries are ready for seamless integration into the AD domain.

V. INTEGRATION WITH SECURITY AND COMPLIANCE ECOSYSTEMS

1. SIEM integration and centralized event logging

CentrifyDC produces detailed logs related to authentication attempts, session activity, and privilege escalations. These logs are essential for security visibility and can be forwarded to Security Information and Event Management (SIEM) systems such as Splunk, QRadar, or ArcSight. Through syslog forwarding and event connectors, Centrify logs become part of the broader security event fabric, allowing analysts to correlate UNIX system activity with enterprise-wide security incidents. This centralization aids in the detection of anomalies and supports compliance with incident response procedures.

2. Compliance alignment and reporting support

Many organizations operating in regulated environments must provide auditable records of access control and user activity. CentrifyDC helps fulfill these requirements by maintaining records of command execution, session duration, and login patterns, all linked to corporate identities in Active Directory. Reports generated from these logs can be formatted to meet the requirements of frameworks such as HIPAA, PCI-DSS, and SOX. These capabilities simplify audits by showing that access was restricted, monitored, and traceable.

3. Multi-factor authentication and adaptive security policies

CentrifyDC extends the security of UNIX systems by enforcing multi-factor authentication (MFA) policies for critical operations or elevated privilege access. For example, an administrator attempting to use sudo on a Solaris host

might be required to provide a second authentication factor, such as a one-time password (OTP) sent via SMS or generated by an authenticator app. Policies can be tailored to context, such as time of day, geographic location, or system criticality, enabling adaptive security controls that balance protection with operational efficiency.

VI. PERFORMANCE, SCALABILITY, AND HIGH AVAILABILITY

1. Agent performance and local caching

The CentrifyDC agent is designed to perform with minimal resource impact. Once installed, it caches credential information and access policies locally, which enables continued authentication even during temporary connectivity issues with Active Directory. This feature is particularly valuable in remote or high-availability environments where transient network disruptions should not impact user access. Cached entries are updated periodically, ensuring access policies remain current while optimizing performance.

2. Load distribution and regional scalability

In large-scale or globally distributed environments, CentrifyDC supports architecture that accommodates regional domain controllers and distributed zones. By leveraging DNS-based Kerberos referrals and Active Directory site topology, authentication traffic can be directed efficiently to the nearest controllers. This regionalization reduces authentication latency and minimizes unnecessary WAN traffic, providing users with fast and reliable access while maintaining centralized control.

3. Monitoring, diagnostics, and resilience planning

Centrify provides diagnostic tools that monitor the status of the agent, AD connectivity, zone policy application, and local cache health. System administrators can use these diagnostics to detect misconfigurations, policy synchronization failures, or performance bottlenecks. Logs and monitoring hooks can also be integrated into enterprise observability platforms for real-time tracking. For resilience, backup configurations, standby domain controllers, and redundant zone mappings can be implemented to support failover scenarios and minimize downtime during maintenance or outages.

VII. USER IDENTITY MAPPING AND ROLE-BASED ACCESS CONTROL

1. Mapping Active Directory users to UNIX identities

CentrifyDC enables seamless identity mapping between Active Directory (AD) users and their UNIX/Linux counterparts. This eliminates the need to maintain separate user databases across systems. When a user logs into a UNIX system, CentrifyDC translates their AD identity into a UNIX user ID (UID), group ID (GID), and home directory path

based on zone-defined rules. This identity mapping ensures consistency in permissions, facilitates single sign-on (SSO), and removes administrative overhead associated with duplicate identity management.

2. Role definition and access scoping

Role-Based Access Control (RBAC) in CentrifyDC allows administrators to define operational roles such as application administrator, database engineer, or system auditor and assign specific command rights, login privileges, and elevation permissions accordingly. These roles are scoped within defined zones and linked to AD security groups. For example, a user in the “Oracle DBA” group may be permitted shell access to Solaris servers and allowed to restart database services, but denied any root-level access on Linux web hosts. This granular policy enforcement ensures principle of least privilege and operational accountability.

3. Time-based and session-aware access controls

CentrifyDC supports temporal controls, restricting access to specific time windows or setting expiration on temporary privileges. This is particularly useful in change management processes or during incident response scenarios where temporary elevated access must be revoked automatically. Additionally, session-aware access allows administrators to monitor active user sessions and, if necessary, terminate or audit them in real time. These controls help mitigate risks posed by stale sessions, unmonitored privilege use, and insider threats.

VIII. OPERATIONAL BENEFITS AND ADMINISTRATIVE SIMPLIFICATION

1. Centralized account lifecycle management

By integrating UNIX account management with Active Directory, CentrifyDC significantly simplifies the user lifecycle process—onboarding, role changes, and offboarding are automatically reflected across all UNIX/Linux systems. When a user is removed from AD or a security group, their access to CentrifyDC-managed systems is revoked instantly, eliminating lingering accounts and access sprawl. This real-time synchronization enhances security posture while reducing manual workload on IT administrators.

2. Simplified sudo policy administration

Traditional sudoers file management is error-prone and lacks centralized oversight. CentrifyDC replaces host-based sudo configurations with centralized policy definitions enforced via zones. Commands that require elevation are associated with roles and AD groups, with audit trails preserved for every action. This approach not only eliminates the need to maintain separate sudoers files on each system, but also ensures compliance with operational and security policies by defining who can run what, when, and where.

3. Enhanced audit readiness and traceability

Through centralized logging of identity mapping, session activity, and command execution, CentrifyDC supports internal audit processes and external regulatory assessments. Logs can be enriched with contextual data like hostname, zone, timestamp, and role applied. These audit trails are exportable to compliance platforms or SIEM solutions, enabling detailed reconstructions of user activity for incident investigations and ensuring adherence to data protection mandates such as HIPAA or SOX.

IX. SECURITY CONSIDERATIONS AND RISK MITIGATION

1. Credential security and protection mechanisms

CentrifyDC ensures that credentials are never stored or transmitted in cleartext. All communication between UNIX agents and Active Directory occurs over encrypted channels using Kerberos or LDAP over TLS. Local caches are protected with file-level encryption, and password policies remain enforced through native AD mechanisms. These practices ensure that enterprise credentials are shielded from exposure, even on older or less secure UNIX platforms.

2. Secure agent deployment and update management

The Centrify agent is packaged with integrity verification and digital signatures, allowing organizations to verify its authenticity before deployment. Updates to the agent can be centrally orchestrated, ensuring consistency across environments. Best practices recommend deploying the agent using privileged package managers or orchestration tools (e.g., Ansible, Puppet) and disabling unnecessary modules to reduce attack surface.

Challenges and Limitations

Dependency on Active Directory availability

While CentrifyDC enhances access control by leveraging Active Directory, it also introduces a dependency on AD’s availability and performance. In cases where the AD infrastructure becomes unreachable—due to network segmentation, domain controller failure, or DNS issues—authentication attempts may fail if local caching is disabled or expired. Although CentrifyDC provides offline login caching, this feature must be carefully managed to avoid authentication delays or denial of access, particularly for systems that rely on real-time AD validation.

Complexity in large-scale zone management

As organizations scale to include hundreds or thousands of servers, managing multiple Centrify zones and role definitions can become increasingly complex. Improperly designed zones may result in redundant policies, conflicting access rights, or gaps in privilege enforcement. This complexity requires skilled administrators who understand the nuances of

Centrify's access model and can balance between granular control and maintainability. Tools for visualizing zone inheritance and auditing role memberships are helpful but may still fall short in extremely large or federated environments.

Compatibility gaps with legacy or niche UNIX variants

Although CentrifyDC supports a broad array of UNIX and Linux distributions, some legacy operating systems or vendor-specific UNIX flavors may lack full compatibility. Older Solaris releases, customized AIX kernels, or unique BSD variants might not support all CentrifyDC features, such as advanced session capture or MFA integration. In such cases, fallback to partial implementations or hybrid access strategies may be necessary, introducing operational inconsistencies and security exceptions that must be documented and mitigated.

Future Enhancements and Development Roadmap

Integration with AI-driven identity analytics

The future of access control lies in intelligence-driven access decisions, and CentrifyDC is positioned to benefit from integrating AI-based identity analytics. These systems can analyze historical login behavior, detect anomalies, and recommend access policies tailored to each user's usage profile. For example, AI engines could dynamically restrict access for a user logging in from an unusual location or performing an abnormal series of commands, adding another layer of contextual protection beyond static roles.

Enhanced support for DevOps and ephemeral workloads

Modern IT environments are rapidly embracing containerized workloads, dynamic virtual machines, and DevOps toolchains. CentrifyDC's roadmap is expected to extend secure access control to ephemeral systems—such as Docker containers or short-lived cloud instances by offering APIs for just-in-time role provisioning, temporary credential injection, and automated de-provisioning. This expansion will allow secure, compliant access to transient systems without sacrificing auditability or increasing administrative burden.

Unified dashboard and cross-domain policy orchestration

Organizations are demanding unified management interfaces that provide visibility and control over access policies across Windows, Linux, UNIX, and cloud systems. Centrify is likely to evolve toward a cross-domain dashboard that consolidates identity policies, session monitoring, audit trails, and compliance reports into a single pane of glass. Such an interface would reduce administrative overhead, streamline reporting, and support policy consistency across a diverse and hybrid enterprise environment.

X. CONCLUSION

CentrifyDC delivers a powerful solution for managing secure access control across heterogeneous UNIX, Linux, and

Windows systems by bridging the gap between traditional UNIX authentication and modern identity governance frameworks. Through tight integration with Active Directory, it provides centralized identity mapping, role-based access control, privileged session monitoring, and comprehensive auditing capabilities—making it especially suitable for enterprises operating in regulated or security-sensitive environments. Its ability to enforce least privilege principles, manage sudo policies centrally, and extend MFA protections to command-level access significantly elevates an organization's security posture. Despite deployment challenges in large or legacy environments, CentrifyDC offers a scalable and adaptable framework that aligns with the future of secure, identity-aware infrastructure management. As IT ecosystems continue to evolve toward hybrid and cloud-native architectures, solutions like CentrifyDC will remain pivotal in achieving secure and compliant access control across distributed and multi-platform environments.

REFERENCES

1. Jaikla, T., Vorakulpipat, C., Rattanalernusorn, E., & Hoang, D. (2019). A Secure Network Architecture for Heterogeneous IoT Devices using Role-based Access Control. 2019 International Conference on Software, Telecommunications and Computer Networks (SoftCOM), 1-5.
2. Boubakri, W., Abdallah, W., & Boudriga, N. (2017). Access control in 5G communication networks using simple PKI certificates. 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), 2092-2097.
3. Tamboli, M.B., & Dambawade, D. (2016). Secure and efficient CoAP based authentication and access control for Internet of Things (IoT). 2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), 1245-1250.
4. Awan, I., & Mellor, J.E. (2007). Performance Analysis of Secure Call Admission Control in Heterogeneous Networks. The 2007 International Conference on Next Generation Mobile Applications, Services and Technologies (NGMAST 2007), 229-234.
5. Li, Z., & Zhou, Y. (2018). Secure and Achievable Heterogeneous Access Control Scheme for Wireless Body Area Networks. International Conference on Foundations of Computer Science.
6. Battula, V. (2021). Dynamic resource allocation in Solaris/Linux hybrid environments using real-time monitoring and AI-based load balancing. International Journal of Engineering Technology Research & Management, 5(11), 81-89. <https://ijetrm.com>
7. Battula, V. (2022). Legacy systems, modern solutions: A roadmap for UNIX administrators. Royal Book Publishers.

8. Madamanchi, S. R. (2021). Disaster recovery planning for hybrid Solaris and Linux infrastructures. *International Journal of Scientific Research & Engineering Trends*, 7(6), 01–08.
9. Madamanchi, S. R. (2021). Linux server monitoring and uptime optimization in healthcare IT: Review of Nagios, Zabbix, and custom scripts. *International Journal of Science, Engineering and Technology*, 9(6), 01–08.
10. Madamanchi, S. R. (2021). Mastering enterprise Unix/Linux systems: Architecture, automation, and migration for modern IT infrastructures. Ambisphere Publications.
11. Madamanchi, S. R. (2022). The rise of AI-first CRM: Salesforce, copilots, and cognitive automation. PhDians Publishers.
12. Mulpuri, R. (2021). Command-line and scripting approaches to monitor bioinformatics pipelines: A systems administration perspective. *International Journal of Trend in Research and Development*, 8(6), 466–470.
13. Mulpuri, R. (2021). Securing electronic health records: A review of Unix-based server hardening and compliance strategies. *International Journal of Research and Analytical Reviews*, 8(1), 308–315.
14. Kim, S.H., Park, S.Y., Choi, K.W., Lee, T., & Kim, D.I. (2020). Backscatter-Aided Cooperative Transmission in Wireless-Powered Heterogeneous Networks. *IEEE Transactions on Wireless Communications*, 19, 7309-7323.
15. Hauge, M., Mjelde, T.M., Holtzer, A., Drijver, F., Velt, R.I., Hegland, A.M., Ørbekk, E., Barz, C., Kirchhoff, J., & Rogge, H. (2020). Inter-network interoperability for heterogeneous networks at the tactical edge. 2020 Military Communications and Information Systems Conference (MilCIS), 1-7.
16. in 't Veld, D., van der Leij, M.J., & Hommes, C.H. (2016). The Formation of a Core-Periphery Structure in Heterogeneous Financial Networks. *Conflict Studies: International Relations Theory eJournal*.
17. Hwang, D., Kim, D.I., Choi, S.K., & Lee, T. (2015). UE Relaying Cooperation Over D2D Uplink in Heterogeneous Cellular Networks. *IEEE Transactions on Communications*, 63, 4784-4796.
18. Kim, S.H., & Kim, D.I. (2019). Backscatter Based Cooperative Transmission in Wireless-Powered Heterogeneous Networks. 2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall), 1-5.
19. Sheshjavani, A.G., Khonsari, A., Shariatpanahi, S.P., Electrical, M.M., Engineering, C., Engineering, C.O., Tehran, U.O., Iran, Science, S.O., & Sciences, I.F. (2021). Content Caching for Shared Medium Networks Under Heterogeneous Users' Behaviours. *ArXiv*, abs/2105.03220.
20. Chen, H., Huang, Y., & Lin, S. (2011). A Generalized Associated Temporal and Spatial Role-Based Access Control Model for Wireless Heterogeneous Networks. 2011 Fifth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, 429-433.
21. Heath, R.W., Debbah, M., Larsson, E.G., Kim, D.I., Viswanathan, H., & Güvenç, I. (2012). Introduction to the Issue on Signal Processing in Heterogeneous Networks for Future Broadband Wireless Systems. *IEEE J. Sel. Top. Signal Process.*, 6, 213-215.
22. Kong, I., & JaeGal, H. (2011). Design of Building System with LED Lighting Control in Heterogeneous Networks. *The Journal of the Korean Institute of Information and Communication Engineering*, 15, 1053-1059.