Leveraging Microsoft Privileged Identity Management Features for Compliance with ISO 27001, PCI, and FedRAMP

December 24, 2015

Coalfire Systems, Inc.
www.coalfire.com

TABLE OF CONTENTS

Contents

Introduction

With emerging cyber threats, Privileged Access Identity is the main target for attackers that want to gain control over an organization's high value assets. To help organizations better secure and manage their privilege access, Microsoft provides a set of solutions that include "Just In Time" administration with Microsoft Identity Manager 2016 and "Just Enough" Administration with Windows Management Framework 5.0. These enable addressing Privileged Identity Management in existing datacenter and private cloud environments. In this paper, we will discuss these new privilege access management solutions and how they can be used to meet compliance requirements present in many business or enterprise information systems.

With proper implementation, these new privilege access management solutions can help organizations transition from a broad access model for administrators to a more restricted, granular access model that better addresses common security issues without compromising operations efficiency, administrator flexibility, or administrative control.

In order to help customers navigate this new capability, Microsoft worked closely with Coalfire, a recognized third-party IT compliance firm, to define each security and compliance objective in relation to the capabilities of JEA and JIT, and provided an example use case for each compliance and security objective. In addition, Appendix A and B contain mappings between JEA and JIT and the security control requirements present in ISO 27001, PCI DSS, and FedRAMP. Although JEA and JIT can be used separately - they provide coverage for many of the same security control requirements – they are most effective when used in tandem.

Overview of 'Just Enough Administration' and 'Just in Time' Privileged Access Management

In any discussion of information system security, one commonly overlooked attack vector is the privileges and access granted to the system administrators themselves. When a system administrator is granted privileged access to an information system, the system security and compliance trust boundary are extended to that user. This represents a real risk; insider attacks and stolen credentials are both real and common.

The question of how to effectively control administrator privileges and limit unnecessary access is not a new problem. Customers are familiar with the principle of least privilege, and may use some form of role based access control (RBAC) with applications that provide it. However, limited scope and large grained control limit the effectiveness and manageability of these solutions. For example, on Servers, privileged access is largely a binary switch, forcing customers to give unnecessary permissions when adding users who perform system administrator duties. In the past, the potential risk involved in this type of access is often rationalized as necessary for business operations.

When analyzing the numerous breaches over the past few years, one quickly concludes that no matter what method was used to breach the environment, the attackers proceed to compromising administrator credentials so that they can integrate, control and hide inside the environment.

In response, Microsoft released two new innovative solutions that help customers deploy an appropriate 'least privilege' access management structure for their entire environment that provides granular access management restrictions for administration tasks.

The first, Just Enough Administration (JEA) delivered as part of the Windows Management Framework 5.0 and supported from Windows Server 2008 R2 and on, provides customers with a robust RBAC platform administered through Windows PowerShell and managed by Windows PowerShell Session Configurations. JEA allows customers to restrict the tasks specific users can perform in relation to specific administrative or privileged duties, without giving the user administrator rights to the entire server or customer environment. For the first time, customers have the ability to manage RBAC with built-in PowerShell functionality, closing numerous loopholes present in older RBAC implementations and simplifying management of RBAC configuration settings.

The second, Just In Time Administration (JIT) delivered in Microsoft Identity Manager 2016, provides customers the ability to assign dynamic privileges to users in existing Windows Server and Active Directory environments to ensure users only have appropriate privileges when necessary and for a limited amount of time. JIT is administered through Microsoft Identity Manager, and can integrate closely with JEA PowerShell configurations to ensure customers have the ability to dynamically allocate privileges and control privileged access from the same PowerShell console.

Both JEA and JIT can be used with multiple versions of Windows Server, including Windows Server 2012 R2 and Windows Server 2008 R2. Customers who implement one or both of these two access management solutions will be able to leverage several important protections that were not previously available in Windows Server.

- First, no user administered under JEA has privileged access to the information system by default.
- Second, when granted administrative privileges using JEA, the user can only perform certain tasks, and they are not full administrators on the server they are managing.
- Third, when someone needs to perform administrative actions, they must request to be an administrator for a set period of time by going through the approval process within JIT that can range from providing automatic approval, or requiring multi-factor authentication or manual approval.
- Finally, with a proper implementation of JEA and JIT, customers can now granularly log all user privilege allocation, approval, and execution throughout the privilege management lifecycle. Administrative actions are now logged from the privilege request workflow to the administrative operations performed on the servers or information system, providing customer the ability to monitor and detect malicious behavior more effectively than ever.

Leveraging JEA and JIT Capabilities for Security and Compliance with ISO 27001, PCI, and FedRAMP

Microsoft designed these features to effectively complement existing customer access control models, Active Directory infrastructure, and enterprise architecture. In addition to providing customers a more powerful and effective way of administering JEA and JIT capabilities, these new access management solutions can also help customers more effectively meet compliance with several common compliance frameworks. The remainder of this document is aimed at providing customers a good idea of control or requirement applicability for these features across three common compliance frameworks: ISO 27001, PCI DSS, and FedRAMP.

Although compliance does not directly equate to security, many customers are required to adhere to different compliance standards as part of doing business. These new access management solutions are broadly applicable to numerous different controls within ISO 27001, PCI DSS, and FedRAMP, and provide customers an easier and more efficient way to meet applicable control requirements that are already in place.

JEA and JIT can help customers navigate three high-priority compliance and security objectives, which constitute the majority of access management control requirements within ISO 27001, PCI DSS, and FedRAMP.

Controlling Logical Access Privileges and Implementing Least Privilege Access

First, JEA and JIT can be used separately or in tandem to provide customers a strong security and compliance posture in relation to the control of logical access privileges and the concept of 'least privilege'. As previously described, JEA and JIT provides the ability to granularly control privilege and access allocation for users. This includes the capability to implement automatic privilege expiration, application or even task-specific privilege restrictions, and strong protections and restrictions in place to enforce privilege restrictions and prevent users from circumventing privilege restrictions.

An example use case for JEA and JIT logical access privilege control and 'least privilege' implementation is as follows: a service provider user needs to periodically reconfigure or patch a Windows Server 2008 R2 server. Instead of being granted blanket system administrator rights for the server, the service provider system manager ensures the user only has access to appropriate privileged commands and functions that permit the user to perform patching and update functions. Prior to deployment, the system manager must complete a predefined elevation workflow to approve the temporary assignment of permissions to the user, which ensures appropriate visibility into the patching activity. Once the user has completed their task, the privileges are revoked to ensure the account cannot be misused or compromised when not in use for that task.

Enforcing Separation of Duties

Second, JEA and JIT can be used separately or in tandem to provide customers the ability to enforce 'separation of duties' within their environments at a much more granular level than was traditionally possible. With DevOps roles becoming more and more common in customer organizations, JEA and JIT capabilities provide customers the ability to ensure development and operations roles can be separated by system function or responsibility, as opposed to blanket system administrator access. This provides clients an effective way to maintain separation of duties controls already in place - which are often heavily emphasized in any compliance review - and apply them to a more flexible, effective DevOps model.

An example use case for JEA and JIT granular ‘separation of duties’ enforcement is as follows: an enterprise is planning a transition to a DevOps model for their internal IT infrastructure and custom applications. In order to adhere to industry security best practices, regulatory requirements, and compliance certifications that dictate strong separation of duties, the enterprise implements JEA and JIT capabilities to control access for the DevOps model. The enterprise ensures all access approvals are manually approved when considered necessary, and are well documented to provide a strong audit trail for any assessors or external auditors. In addition, the enterprise ensures that access is limited to specific functions to control the scope of their potential actions on the system and prevent any perceived violation of separation of duties requirements.

Access Logging / Monitoring / Auditing

Finally, with JEA and JIT customers can now granularly log all user privilege allocation, approval, and execution throughout the privilege management lifecycle. Administrative actions are now logged from the privilege request workflow to the administrative operations performed on the servers or information system, providing customer the ability to monitor and detect malicious behavior more effectively than ever.

An example use case for JEA and JIT access and privilege allocation logging and monitoring is as follows: a customer user must perform a highly sensitive action within the information system. JIT/JEA will allow for the automation of increased logging and monitoring levels during privileged operations such as a change management task.

Appendix A: Just Enough Administration Compliance Mapping to ISO 27001, PCI, and FedRAMP

JEA Security and Compliance Capability	ISO 27001: 2013	PCI DSS 3.1	FedRAMP; NIST 800-53 Revision 4
Controlling Logical Access Privileges and Implementing Least Privilege Access	A.9.1 – Business requirement of access control A.9.1.2 – Access to networks and network services A.9.2.2 – User access provisioning A.9.2.3 – Management of privileged access rights A.9.4.1 – Information access restriction A.9.4.5 – Access control to program source code	7.1 – System components and cardholder data access restricted to job-based needs 7.1.1 – Define role access needs 7.1.2 – User ID access based on least privileges 7.1.3 – Assigning access to job function and classification 7.1.4 – Documented approval of access privileges 7.2 – User access control on need-to-know basis 7.2.2 – Assigning privileges to job function and classification 7.2.3 – Default "deny-all" setting 12.5.4 – Administer user accounts 12.5.5 – Monitor and control all access to data	AC-2 – Account Management AC-2 (7) – Account Role-Based Schemes AC-3 – Access Enforcement AC-6 – Least Privilege AC-6 (1) – Authorize Access to Security Functions AC-6 (2) – Non-Privileged Access for Non-Security Functions AC-6 (5) – Privileged Accounts AC-6 (10) – Prohibit Non-Privileged Users from Executing Privileged Functions AU-9 (4) – Audit Access by Subset of Privileged Users CM-5 – Access Restrictions for Change CM-5 (1) – Automated Access Enforcement CM-5 (5) – Limit Production / Operational Privileges
Enforcing Separation of Duties	A.6.1.2 – Segregation of duties A.12.1.4 – Separation of development, testing, and operational environments	6.4.2 – Separation of duties between test and production environments	AC-5 – Separation of Duties
Access Logging / Monitoring / Auditing	A.12.4.1 – Event logging	10.2.2 – Logging actions by root privileges individual	AC-2 – Account Management AC-2 (4) – Automated Audit Actions

JEA Security and Compliance Capability	ISO 27001: 2013	PCI DSS 3.1	FedRAMP; NIST 800-53 Revision 4
	A.12.4.3 – Administrator and operator logs	10.2.5 – User changes logging 12.5.5 – Monitor and control all access to data	AC-2 (12) – Account Monitoring AC-6 (9) – Auditing Use of Privileged Functions AU-2 – Audit Events AU-12 – Audit Generation CM-5 (1) – Automated Access Enforcement

Appendix B: Just In Time Administration Compliance Mapping to ISO 27001, PCI, and FedRAMP

JIT Security and Compliance Capability	ISO 27001: 2013	PCI DSS 3.1	FedRAMP; NIST 800-53 Revision 4
Controlling Logical Access Privileges and Implementing Least Privilege Access	A.9.1 – Business requirement of access control A.9.1.2 – Access to networks and network services A.9.2.2 – User access provisioning A.9.2.3 – Management of privileged access rights A.9.4.1 – Information access restriction A.9.4.5 – Access control to program source code	7.1 – System components and cardholder data access restricted to job-based needs 7.1.2 – User ID access based on least privileges 7.1.3 – Assigning access to job function and classification 7.1.4 – Documented approval of access privileges 7.2.2 – Assigning privileges to job function and classification 7.2.3 – Default “deny-all” setting 12.5.4 – Administer user accounts 12.5.5 – Monitor and control all access to data	AC-2 – Account Management AC-3 – Access Enforcement AC-6 – Least Privilege AC-6 (1) – Authorize Access to Security Functions AC-6 (2) – Non-Privileged Access for Non-Security Functions AC-6 (5) – Privileged Accounts AU-9 (4) – Audit Access by Subset of Privileged Users CM-5 – Access Restrictions for Change CM-5 (1) – Automated Access Enforcement CM-5 (5) – Limit Production / Operational Privileges
Access Logging / Monitoring / Auditing	A.12.4.1 – Event logging A.12.4.3 – Administrator and operator logs	10.2.2 – Logging actions by root privileges individual 10.2.5 – User changes logging	AC-2 – Account Management AC-2 (4) – Automated Audit Actions AC-2 (12) – Account Monitoring AC-6 (9) – Auditing Use of Privileged Functions AU-2 – Audit Events AU-12 – Audit Generation CM-5 (1) – Automated Access Enforcement