International Journal of Information Technology (IJIT)
Volume 4, Issue 02, July-December 2023, pp. 29-37 Article ID: IJIT_4_02_004
Available online at https://iaeme.com/Home/issue/IJIT?Volume=4&Issue=2
Journal ID: 4573-3410

ACTIVE DIRECTORY IMPLEMENTATION: RESOLVING PROVISIONING / DEPROVISIONING ACCESS AND ENSURING ACCURATE USER IDENTITY AND ACCESS ACROSS THE ORGANIZATION USING IAM

Sampath Talluri
Department of Computer Science, Western Michigan University,
1903 W Michigan Ave, Kalamazoo, MI 49008, United States

Vamsy Priya Anne
Department of Computer Information Systems,
Grand Valley State University, 1 Campus Dr, Allendale, MI 49401, United States

ABSTRACT

Background: *Managing user identities and access rights in organizations is a parliament activity to ensure data security and operational efficacy. Identity and Access Management (IAM) tools are the best solution.*

Methods: *This research presents a detailed implementation of an Active Directory (AD) solution to resolve synchronization issues, streamline access provisioning and de-provisioning processes, and fortify user identity and access accuracy.*

Results: *Leveraging advanced IAM tool synchronization jobs, automation, and role-based access control (RBAC) is crucial to every organization.*

Conclusion: *The implementation yielded substantial improvements in efficiency and accuracy. IAM is a critical tool in today's interconnected and digital world. Organizations need help with challenges, such as how to efficiently and securely manage the accounts and access of their employees, contractors, and stakeholders. The Joiner, Mover, and Leaver (JML) process has a crucial framework within IAM to tackle user lifecycle challenges head-on. It is a comprehensive approach to managing user access throughout their role within an organization.*

Keywords: Active Directory (AD), Provisioning, De-provisioning, Synchronization, Identity and Access Management (IAM), Users, Access, Roles.

Cite this Article: Sampath Talluri and Vamsy Priya Anne, Active Directory Implementation: Resolving Provisioning / Deprovisioning Access and Ensuring Accurate User Identity and Access Across the Organization Using IAM, *International Journal of Information Technology (IJIT)*, 4(2), 2023, pp. 29-37
https://iaeme.com/Home/issue/IJIT?Volume=4&Issue=2

1. BACKGROUND

Active Directory (AD) is the backbone for managing user identities and access privileges within organizational IT infrastructures. The complex users, access, roles, and the growth of Hybrid and Cloud-based services require robust AD implementation to address synchronization challenges and optimize access management using the IAM tools.

The existing Active Directory system faced discrepancies in synchronization, leading to user identity, access, data inaccuracies, and manual intervention. Posed operational challenges and increased security risks due to inconsistent user and access provisioning and de-provisioning.

This paper explores the critical aspects of managing fine-tuned access to the accounts within Active Directory. By the end of this paper, readers will have a comprehensive understanding of the IAM tools, permissions, use cases, and procedures required to effectively provision and de-provision access, ensuring security and operational efficiency.

The Primary Objectives of this Implementation:

Resolving synchronization issues in the Active Directory system is crucial to maintaining consistent and up-to-date user identity and access data across the network. Which involves troubleshooting issues related to replication, ensuring that changes made in one domain controller are appropriately synchronized with others, and resolving conflicts that may arise during this process.

Streamlining provisioning and de-provisioning access processes using Identity and Access Management (IAM) tools enhances security and efficiency. These tools automate user onboarding and offboarding, reducing the risk of human error and ensuring that users have the right level of access during their tenure with the organization.

Ensuring the accuracy of user identity and access synchronization across the entire organization is vital for security and compliance. This means that users have appropriate access permissions and that these permissions are consistently maintained and audited to prevent unauthorized access and data breaches.

Risks and challenges associated with inappropriate access provisioning and de-provisioning include security breaches, data leaks, compliance violations, and resource wastage. Inadequate control over user access can lead to unauthorized access, which can have significant financial, legal, and reputational consequences for an organization.

Implementing practical IAM tools and synchronization processes can greatly assist compliance and audit teams by providing a robust framework for managing access and tracking user activities. This ensures that the organization can meet regulatory requirements, maintain a clear audit trail, and quickly respond to audit requests, thus bolstering its overall compliance posture.

2. METHODS

The Active Directory system was upgraded to incorporate advanced synchronization mechanisms, including real-time user accounts and Access synchronization in a Hybrid environment Figure 1. Integration with third-party (IAM) tools enhanced the overall functionality, providing a robust foundation for improved identity and access management solutions.

Figure 1: Architecture Diagram

The implementation involved the integration of the IAM solution and real-time synchronization rules in identifying and resolving discrepancies promptly in the target system. Account Mapping is used in the IAM used in Figure 2.

```
[ACCOUNTID::distinguishedName#String,
NAME::sAMAccountName#String,
InCorrectLogons::logonCount#String,
VALIDTHROUGH::accountExpires#millisec, ACCOUNTCLASS::objectClass#String,
CUSTOMPROPERTY1::Name#String,
CustomProperty2::employeeID#String,
CustomProperty3::userPrincipalName#String, CUSTOMPROPERTY4::objectGUID#Binary,
CustomProperty5::facsimileTelephoneNumber#String,
CUSTOMPROPERTY7::givenName#String, CUSTOMPROPERTY8::l#String,
CUSTOMPROPERTY9::mail#String,
CUSTOMPROPERTY10::mobile#String,
CUSTOMPROPERTY11::sn#String,
CUSTOMPROPERTY12::co#String, CUSTOMPROPERTY13::company#String,
CUSTOMPROPERTY14::Department#String,
CUSTOMPROPERTY15::businessCategory#String,
CUSTOMPROPERTY16::employeeType#String, CUSTOMPROPERTY17::postalCode#String,
CUSTOMPROPERTY18::HomeDrive#String,
CUSTOMPROPERTY19::ipPhone#String,
CUSTOMPROPERTY20::manager#String, CUSTOMPROPERTY21::Office#String,
CUSTOMPROPERTY22::title#String,
CUSTOMPROPERTY23::streetAddress#String,
CUSTOMPROPERTY24::telephoneNumber#String, CUSTOMPROPERTY25::st#String,
CUSTOMPROPERTY26::AccountExpirationDate#date,
CUSTOMPROPERTY50::userAccountControl#number,
STATUS::userAccountControl#Number, CREATED_ON::whenCreated#Date,
UpdateDate::whenChanged#Date,
DISPLAYNAME::displayName#String,
LASTLOGONDATE::lastLogonTimestamp#Date,
LASTPASSWORDCHANGE::pwdLastSet#millisec, RECONCILATION_FIELD::ACCOUNTID,
CustomProperty27::nspmDistributionPassword#String,
CustomProperty28::description#String, CustomProperty29::physicalDeliveryOfficeName#String,
CustomProperty30::primarytelexnumber#String,
CustomProperty33::msDS-cloudextensionAttribute7#String, CustomProperty32::extensionAttribute2#String,
CustomProperty31::proxyAddresses#String,
CustomProperty34::c#String,
CustomProperty35::extensionattribute11#String,
CustomProperty36::extensionattribute9#String,CustomProperty37::initials#String,
CustomProperty38::otherIpPhone#String,
CustomProperty39::extensionAttribute8#String,
CustomProperty40::msExchRecipientDisplayType#String,
CustomProperty41::msExchRecipientTypeDetails#String,
CustomProperty42::targetAddress#String,
CustomProperty43::msExchUsageLocation#String,
CustomProperty45::manager#String,
CustomProperty46::lockoutTime#millisec,
CustomProperty47::extensionAttribute12#String
]
```

Figure 2: Account Attribute Mapping from AD to IAM

The status value we are mapping is based on the status we are getting in the reconciliation field [2][5].

Figure 3: Status Config of Accounts

I used the memberOf attribute to pull groups from target AD to IAM. AD will not store the primary GroupID in memberOf but stores it separately in the primaryGroupID attribute.

Figure 4: Group attribute mapping

I am also Importing AD groups based on objectGUID [2]

Figure 5: Group attribute mapping with GUID

To Import the entitlement owners during access import, use entitlementOwnerAttribute [2]

Figure 6: Group attribute mapping along with Owner

Access management was streamlined by introducing automation tools. Principles were applied to categorize users into groups and roles, ensuring access privileges aligned with organizational responsibilities. Users can also request access using the IAM tool, which can be automated after the approval. Figure 7 will give an overview of the fields in which we operate in AD and IAM. The left attributes are from AD, and the Right is from IAM [4]. Figure 8 is used to remove the user access, move the user to a disabled OU, and set a random password for this account.

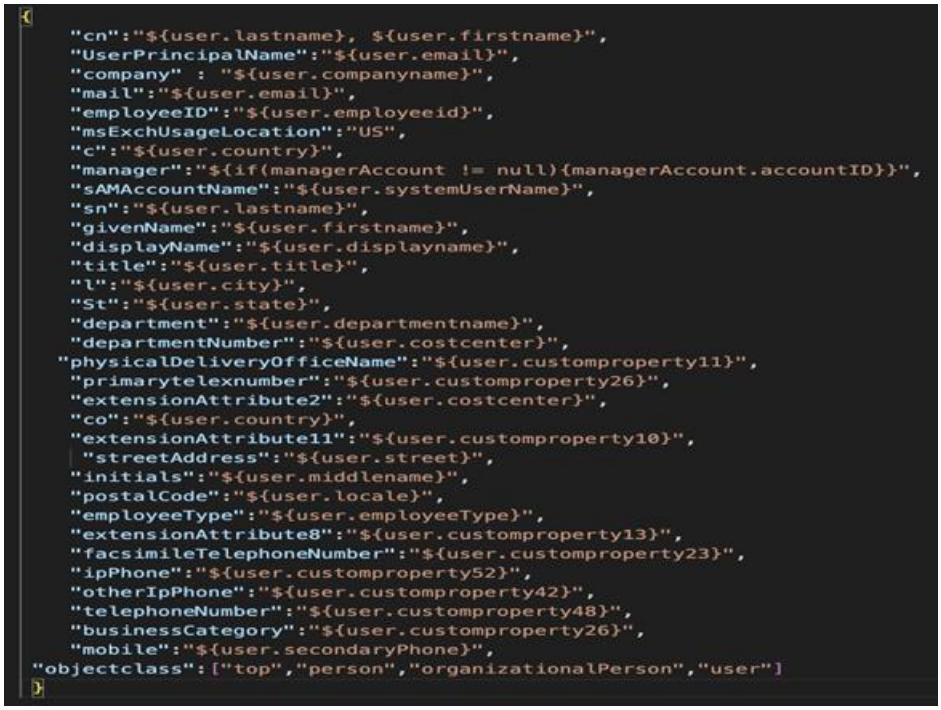


Figure 7: Create/Update Account JSON

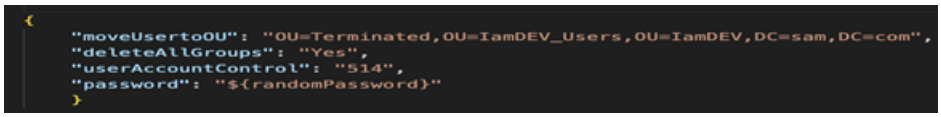


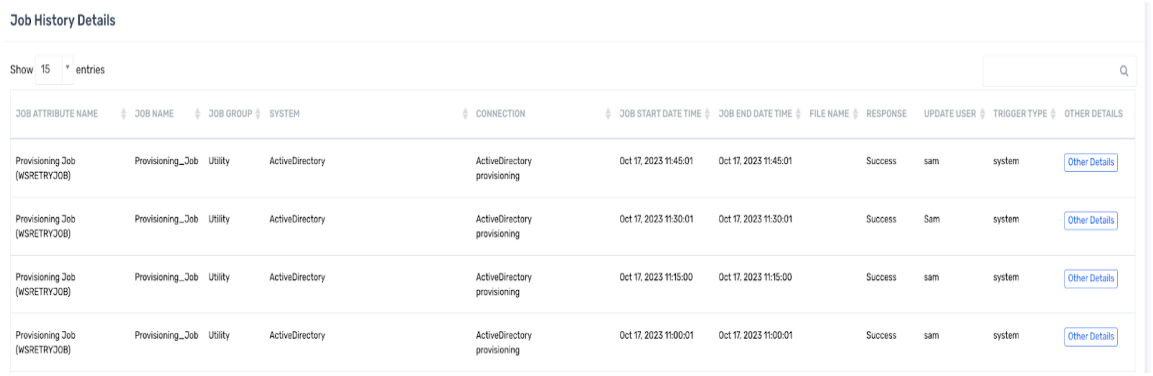
Figure 8: Disable Account JSON

Implementing real-time synchronization Jobs significantly improved synchronization accuracy [8]. Conflicts were proactively identified and resolved, leading to a complete reduction in synchronization discrepancies. If you look at Figures 2,3 and 4, we are using those fields to sync and reconcile the account from target AD to IAM [2]

Access provisioning and de-provisioning processes are automated using the scheduled jobs to expedite the access management process [8]. RBAC principles ensured that users received appropriate access privileges by the time of joining the organization, contributing to a vast increase in efficiency in access management. The user will have all the necessary access. Managers will have complete control of the user permissions and have a clear picture of user access review.

RESULTS

Implementing an IAM tool in an organization has enhanced AD access provisioning and de-provisioning efficiency. This automated approach has streamlined user account creation and access assignment, minimizing manual operations and reducing the risk of human errors. The automation helps quicken onboarding for new employees and ensures efficient access removal for terminating users, contributing to a more agile and responsive IT infrastructure. Regular monitoring and updates to access policies ensure ongoing alignment with organizational needs and security standards.



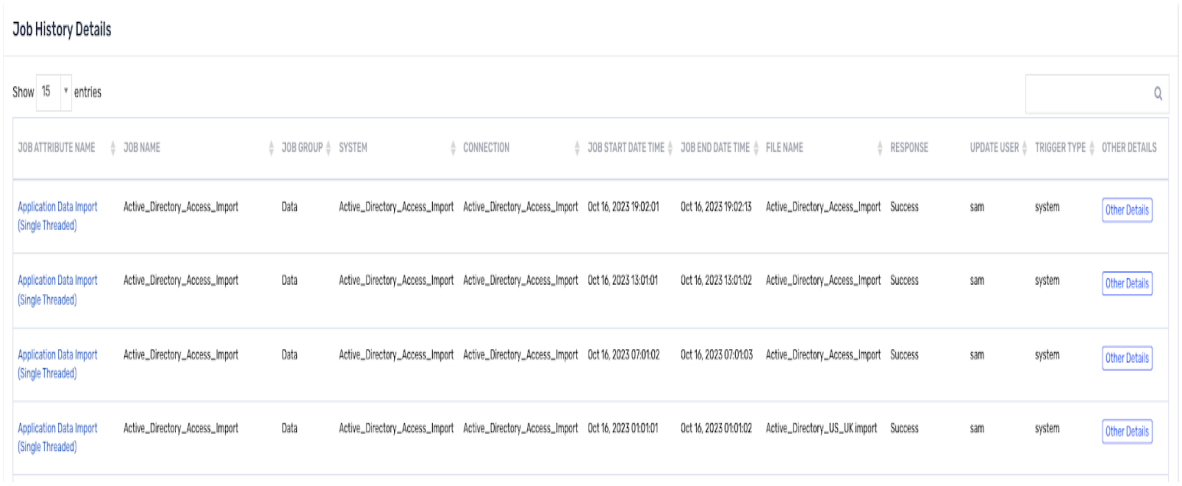
Job History Details

Show 15 entries

JOB ATTRIBUTE NAME	JOB NAME	JOB GROUP	SYSTEM	CONNECTION	JOB START DATE TIME	JOB END DATE TIME	FILE NAME	RESPONSE	UPDATE USER	TRIGGER TYPE	OTHER DETAILS
Provisioning Job (WSRETRYJOB)	Provisioning_Job	Utility	ActiveDirectory	ActiveDirectory provisioning	Oct 17, 2023 11:45:01	Oct 17, 2023 11:45:01		Success	sam	system	Other Details
Provisioning Job (WSRETRYJOB)	Provisioning_Job	Utility	ActiveDirectory	ActiveDirectory provisioning	Oct 17, 2023 11:30:01	Oct 17, 2023 11:30:01		Success	Sam	system	Other Details
Provisioning Job (WSRETRYJOB)	Provisioning_Job	Utility	ActiveDirectory	ActiveDirectory provisioning	Oct 17, 2023 11:15:00	Oct 17, 2023 11:15:00		Success	sam	system	Other Details
Provisioning Job (WSRETRYJOB)	Provisioning_Job	Utility	ActiveDirectory	ActiveDirectory provisioning	Oct 17, 2023 11:00:01	Oct 17, 2023 11:00:01		Success	sam	system	Other Details

Figure 9: Provisioning/De-provisioning Job Results

Leveraging an IAM tool for AD has significantly improved synchronization efficiency, mitigating data discrepancies and bolstering system reliability. Real-time data synchronization from the IAM tool ensures that users are updated promptly in the AD, and maintaining precision and consistency across systems has become efficient. If you look at the Figures 10 & 11. Account synchronization occurs in real time, delivering immediate access adjustments. Further, regular reconciliation processes, conducted every couple of hours from AD to the IAM platform, further enhance reliability by capturing any changes in the AD and updating the IAM tool accordingly. This robust synchronization framework minimizes discrepancies and ensures that the IAM tool remains in sync with the dynamic changes within the AD environment, contributing to a seamless and reliable user management system. Also, ensure the sync/changes from the Human Resource Management System (HRMS) are synced in AD.

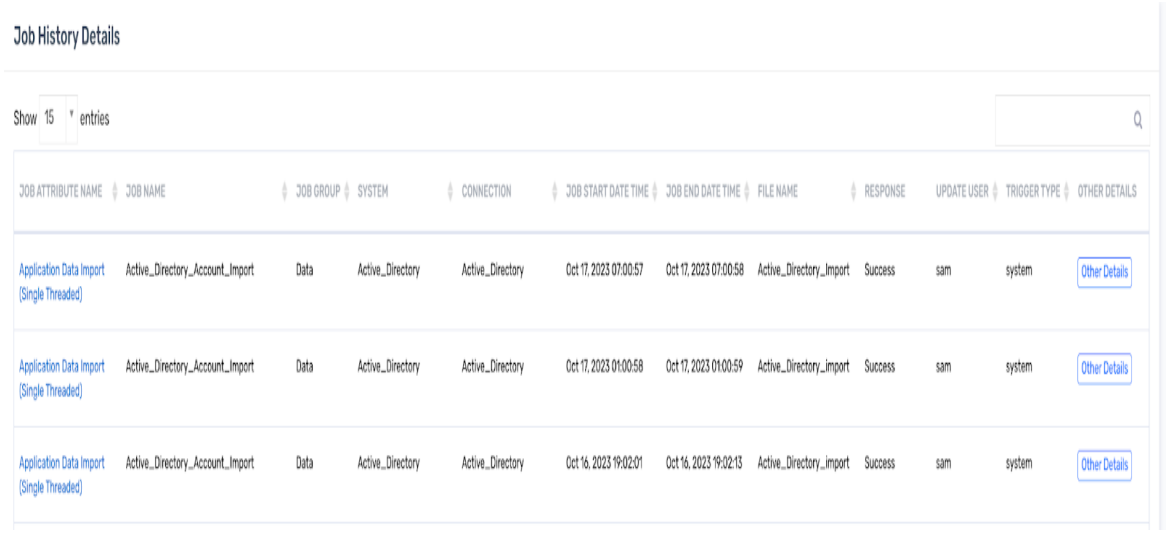


Job History Details

Show 15 entries

JOB ATTRIBUTE NAME	JOB NAME	JOB GROUP	SYSTEM	CONNECTION	JOB START DATE TIME	JOB END DATE TIME	FILE NAME	RESPONSE	UPDATE USER	TRIGGER TYPE	OTHER DETAILS
Application Data Import (Single Threaded)	Active_Directory_Access_Import	Data	Active_Directory_Access_Import	Active_Directory_Access_Import	Oct 16, 2023 19:02:01	Oct 16, 2023 19:02:13	Active_Directory_Access_Import	Success	sam	system	Other Details
Application Data Import (Single Threaded)	Active_Directory_Access_Import	Data	Active_Directory_Access_Import	Active_Directory_Access_Import	Oct 16, 2023 13:01:01	Oct 16, 2023 13:01:02	Active_Directory_Access_Import	Success	sam	system	Other Details
Application Data Import (Single Threaded)	Active_Directory_Access_Import	Data	Active_Directory_Access_Import	Active_Directory_Access_Import	Oct 16, 2023 07:01:02	Oct 16, 2023 07:01:03	Active_Directory_Access_Import	Success	sam	system	Other Details
Application Data Import (Single Threaded)	Active_Directory_Access_Import	Data	Active_Directory_Access_Import	Active_Directory_Access_Import	Oct 16, 2023 01:01:01	Oct 16, 2023 01:01:02	Active_Directory_US_UK import	Success	sam	system	Other Details

Figure 10: Provisioning/De-provisioning Job Results.


Job History Details

Show 15 entries

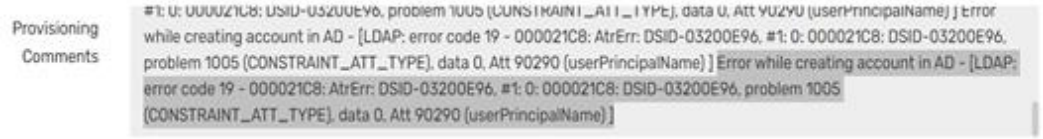
JOB ATTRIBUTE NAME	JOB NAME	JOB GROUP	SYSTEM	CONNECTION	JOB START DATE TIME	JOB END DATE TIME	FILE NAME	RESPONSE	UPDATE USER	TRIGGER TYPE	OTHER DETAILS
Application Data Import (Single Threaded)	Active_Directory_Account_Import	Data	Active_Directory	Active_Directory	Oct 17, 2023 07:00:57	Oct 17, 2023 07:00:58	Active_Directory_Import	Success	sam	system	Other Details
Application Data Import (Single Threaded)	Active_Directory_Account_Import	Data	Active_Directory	Active_Directory	Oct 17, 2023 01:00:58	Oct 17, 2023 01:00:59	Active_Directory_import	Success	sam	system	Other Details
Application Data Import (Single Threaded)	Active_Directory_Account_Import	Data	Active_Directory	Active_Directory	Oct 16, 2023 19:02:01	Oct 16, 2023 19:02:13	Active_Directory_import	Success	sam	system	Other Details

Figure 11: Account and Access Reconciliation Results

4. DISCUSSION ON CHALLENGES AND SOLUTIONS

When implementing this solution, we encountered several challenges, including data conflicts, permissions, and integration issues. These were addressed through rigorous testing, stakeholder collaboration, and troubleshooting calls.
Example:

1. Permission needs to be included for the service account. When creating a user/group in AD [6]


Provisioning Comments

#1: 0: 000021C8: DSID-03200E96, problem 1005 (CONSTRAINT_ATT_TYPE), data 0, Att 90290 (userPrincipalName)] Error while creating account in AD - [LDAP: error code 19 - 000021C8: AtrErr: DSID-03200E96, #1: 0: 000021C8: DSID-03200E96, problem 1005 (CONSTRAINT_ATT_TYPE), data 0, Att 90290 (userPrincipalName)] Error while creating account in AD - [LDAP: error code 19 - 000021C8: AtrErr: DSID-03200E96, #1: 0: 000021C8: DSID-03200E96, problem 1005 (CONSTRAINT_ATT_TYPE), data 0, Att 90290 (userPrincipalName)]

Figure 12: Error while creating the user.

Delete/Disabling operation is not allowed for insufficient permissions.


Provisioning Comments

Deleting/Disabling the Account from AD - [LDAP: error code 50 - 00002098: SecErr: DSID-031514A0, problem 4003 (INSUFF_ACCESS_RIGHTS), data 0] Error while Delete operation for account-aloeffler in AD, Error Deleting/Disabling the Account from AD - [LDAP: error code 50 - 00002098: SecErr: DSID-031514A0, problem 4003 (INSUFF_ACCESS_RIGHTS), data 0] Error while Delete operation for account-aloeffler in AD, Error Deleting/Disabling the Account from AD - [LDAP: error code 50 - 00002098: SecErr: DSID-031514A0, problem 4003 (INSUFF_ACCESS_RIGHTS), data 0]

Figure 13: Error while deactivating account.

2. The account creation issue is resolved after the changes in the values in ‘c’ (CountryName) [6]
3. Delete/Disabling is resolved after providing the necessary permissions to the service account [7]

Figure 14: Successfully provisioned account

5. CONCLUSION

In conclusion, integrating Active Directory (AD) with Identity and Access Management (IAM) systems, complete with synchronization and automated provisioning/de-provisioning processes, presents a comprehensive solution for organizations. This strategic alignment streamlines user management, centralizing control for uniformity and reducing the risk of errors. Automation in provisioning and de-provisioning ensures efficient user lifecycle management, promoting operational productivity.

These IAM solutions contribute to compliance adherence, regulatory requirements, and inherent auditing capabilities. It will also help the organization manage the user identity under a single platform. This integration improves scalability and adaptability and positively impacts the end-user experience with instance Access and features like single sign-on. The resulting improvements in user identity and access data accuracy contribute significantly to the overall efficiency and security of the organizational IT infrastructure.

6. ABBREVIATIONS

AD Active Directory; IAM, Identity and Access Management; IT, Information Technologies; RBAC, Role Based Access Control; OU, Organizational Unit; DC, Domain Controller; GUID, Globally Unique Identifier; HRMS, Human Resource Management System;

7. COMPETING INTERESTS

Not Applicable.

8. FUNDING

Not Applicable.

9. AVAILABILITY OF DATA AND MATERIALS

Not Applicable.

10. AUTHORS' CONTRIBUTIONS

ST designed contributed to this research, and implementation, carried out the experiments, and drafted the Manuscript. VPA helped in the research coordination. The Authors read and approved the final manuscript.

ACKNOWLEDGMENTS

Not Applicable.

REFERENCES

[1] Martinekuan, "Integrate on-premises AD domains with Azure AD - Azure Architecture Center," learn.microsoft.com. https://learn.microsoft.com/en-us/azure/architecture/reference-architectures/identity/azure-ad

[2] "Saviynt Documentation," docs.saviyntcloud.com. https://docs.saviyntcloud.com/bundle/AD-v23x/page/Content/Configuring-the-Integration-for-Importing-Users.htm (accessed Oct. 19, 2022).

[3] "Saviynt Documentation," docs.saviyntcloud.com. https://docs.saviyntcloud.com/bundle/AD-v23x/page/Content/Configuring-the-Integration-for-Importing-Accounts-and-Access.htm (accessed Oct. 19, 2022).

[4] "Saviynt Documentation," docs.saviyntcloud.com. https://docs.saviyntcloud.com/bundle/AD-v23x/page/Content/Configuring-the-Integration-for-Provisioning-and-Deprovisioning.htm (accessed Oct. 19, 2022).

[5] Deland-Han, "User Account Control property flags - Windows Server," learn.microsoft.com, Feb. 23, 2022. https://learn.microsoft.com/en-us/troubleshoot/windows-server/identity/useraccountcontrol-manipulate-account-properties

[6] "Support," knowledge.informatica.com, May 18, 2022. https://knowledge.informatica.com/s/article/325362?language=en_US (accessed Oct. 19, 2022).

[7] "Saviynt Documentation," docs.saviyntcloud.com, May 30, 2022. https://docs.saviyntcloud.com/bundle/AD-v23x/page/Content/Preparing-for-Integration.htm (accessed Oct. 19, 2022).

[8] "Saviynt Documentation," docs.saviyntcloud.com, May 30, 2022. https://docs.saviyntcloud.com/bundle/AD-v23x/page/Content/Import-Recommendations.htm (accessed Oct. 19, 2022).

Citation: Sampath Talluri and Vamsy Priya Anne, Active Directory Implementation: Resolving Provisioning / Deprovisioning Access and Ensuring Accurate User Identity and Access Across the Organization Using IAM, International Journal of Information Technology (IJIT), 4(2), 2023, pp. 29-37

Article Link:
https://iaeme.com/MasterAdmin/Journal_uploads/IJIT/VOLUME_4_ISSUE_2/IJIT_4_02_004.pdf

Abstract:
https://iaeme.com/Home/article_id/IJIT_4_02_004

editor@iaeme.com