*International Journal of Business & Management Study – IJBMS 2018*
*Copyright © Institute of Research Engineers and Doctors , SEEK Digital Library*
*Volume 5 : Issue 1 - [ISSN : 2372-3955] - Publication Date: 25 June, 2018*

# *Centralized Users Management to Access System*

## *Creating Domain ID's and Domain IP's to Access in Centralized Corporate Server.*

[Usman Uz Zaman[1] and Asif Kamran[2]]

***Abstract*** — This study is to examine the Management science in the field of Information Security and Domain Admins. These departments have all access control of the corporate organization by this model research in which 4 variables are defined as dependent variable upon management who controls Networks, System applications, manages infrastructure, creating Servers where Domain ID's and IP's are being created through MS-windows tool for creating access credential by rule of the IP's which was created in designed areas, regions, zone and main office to give right User Identity. The given information by this model, Groups created were to predict for which access security is to define for users role and privilege to Centralized applications and Log-in Access to server which is connected to server based applications for logs save and all activity logs from one centralized backup server**.**

***Keywords—(Managing users group, Passwords, Domain policies, Department rights policies)***

***Introduction***

This Research applies through MS- windows Active Directory support application tool for the management to control all systems with multiple units and departments, to enable assigned policy created for applications and digital information. As to enable information and digital with support of Active Directory Admin groups and organizational units (OU) are created with in the OU and certain IP is directed to the common domain name. Domain policy and settings allows a system to work accordingly by the organizational works policy which would be activated through Windows Server 2008 Group Policy to manage configurations for groups of computers and users. Active Directory Admin who creates policies and organizational units for assigned users created in the directory and controlled by Admin of the organization. The registry-based policy settings, security settings, software deployment and scripts are included an option for groups of users for group policy to manage all configurations. Work policy may be defined within the department or controlled by higher management. In this introduction we discuss creating and managing groups account, how is affected by domain functional level save and secure after creating and managing users. This scenario proves, storing all necessary data on a domain will be safe and secure from unnecessary traffics or hacking prevent damage as it is to be protected safely by firewalls and VPN to be confidential. Domain is managed by a small group of enterprise to manage users and give access for digital applications to manage and control on it, Enterprise and information security admin manages security on user's data and access (accounts, policies, codes and passwords) to enable log for software deployment and script within system.

**Authors Name[1]/ Usman Uz Zaman**

Management Science Department. Institute of Business & Technology Karachi, Pakistan

**Authors Name[2]/ Asif Kamran**

Management Science Department. Institute of Business & Technology Karachi, Pakistan

***Statement of problem***

**This study states the corporate strategy to build secure management.**

The Problems, which a Management or an Admin has to look and solve is to keep maintaining the organization's infrastructure save and secure. There are several traffics, viruses and bad files are to prevent damage to the internal settings or organizational confidential data.

There are only a few possibilities of keeping the infrastructure secure from unnecessary traffics or hacking prevent damage as it is to be protected by firewalls. In addition, you logged onto organization VPN network and a VPN IP address is to be confidential and under assigned otherwise not granted access. Strict firewall rules also applies inside the infrastructure, allowing only assigned IP within the organization through managed by network supports by DNS, especially between servers and work stations (Administrators). Child domains are also strictly separated. There is no need for them as they are accessible in the root domain which is local and forest work. There is auto generate scripts which generate logs, warning errors after bad log-in (bad user name or Password ) via email or by script into log details.

**OBJECTIVES OF THE STUDY:**

Contribution: To present absent voice by using technology contribution in management comprehensively manage and proficiency to secure centralized access control management.

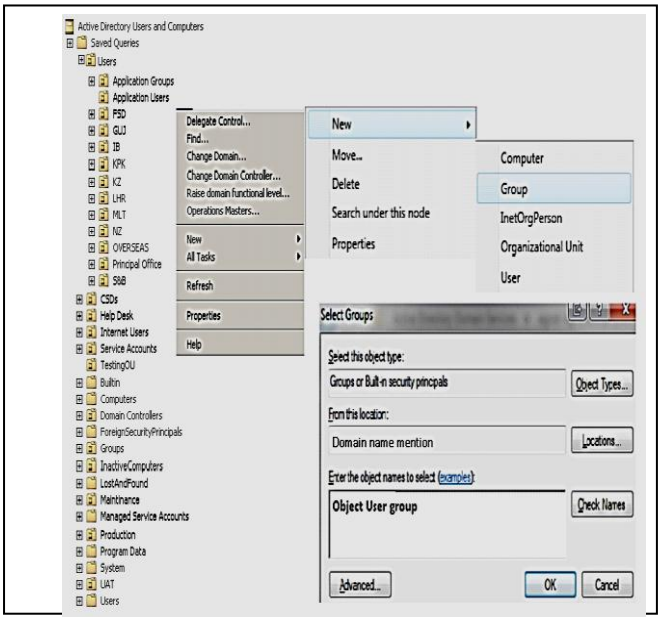
Specific Objectives of research:

- Effectively manage and control on a user access log-in credential.
- Periodic intervals on user access.
- Effective networks monitoring and manage infrastructure with assigned IP addresses through DNS and DHCP.
- Role-based access control on application by giving rights to execute.
- Act under policy assigned to user's Domain.
- Users with their privileges logs are being updated backups created on each critical databases.
- Access control SOP/Policy.
- Procedure for changing/revoking user access.

**RESEARCH METHOD AND PROCEDURE**

This research method defines authentic source applications in this view that manager who implement an infrastructure takes control on accessible credentials by building domain controller on a server could be on 2012 R2 server, as Testing strategy- setting server, cabled, power-up Domain Server as Testing Organization and sets administrative tools operating system(OS) Domain with contained license have administrative powers to set groups, policies, allowing IP's, Creating ID's, passwords, applications, OU and group policy to manage configurations for groups of computers and users.

**RESEARCH DESIGN AND METHOD**




Fig#01 **Active Directory managing users and computer system**

The above figure provides us the complete overview of all the users, groups and security policies that can be propagated through a secure entity. This scheme will not only help us maintaining the authentication of users via a secure channel, but we can save all backup root to centralized confidential servers to maintain backup server and to saves all transactional logs as well by the

Management.

| USERS Management | | | | |
|---|---|---|---|---|
| | frequency | percent | valid percent | cumulative percent |
| STRONGLY AGREE | 50 | 50 | 50 | 50 |
| AGREE | 49 | 49 | 49 | 99 |
| STRONGLY DISAGREE | 1 | 1 | 1 | 100 |
| DISAGREE | 100 | 100 | 100 | |

Table#01 Management will become confident after ease control on domain access privilege.

| ACTIVE DIRECTORY | | | | |
|---|---|---|---|---|
| | frequency | percent | valid percent | cumulative percent |
| STRONGLY AGREE | 43 | 43 | 43 | 43 |
| AGREE | 53 | 53 | 53 | 96 |
| STRONGLY DISAGREE | 2 | 2 | 2 | 98 |
| DISAGREE | 2 | 2 | 2 | 100 |
| TOTAL | 100 | 100 | 100 | |

Table#02 Active Directory to enable management to control on objects.

**2.2 RESPONDANTS OF THE STUDY**

DNS (Domain Name System) would get activated from the authenticated system source from network frame setting that enable respondent area of network. DNS is a protocol that it works within the set of standards for how computers exchange data on the Internet or in centralized area of policy and on many private networks, known as the TCP/IP protocol suite.

**From this above section DNS & DHCP more often defines that each client will be using a DHCP IP that allows them to go through a DHCP server.**

**DHCP server assigns IP address from the pool of ID address gateway.**

**DHCP server defines a range of IP address.**

**Example: Gateway IP 192.168.1.1 / IP ADD range 192.168.1.1 – 50**

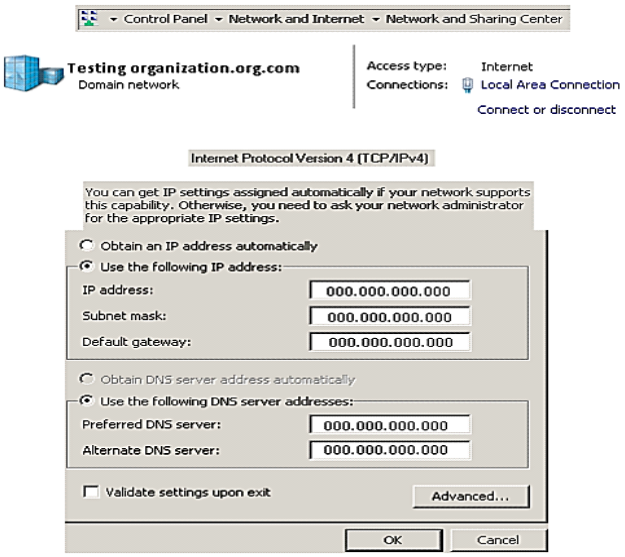
| DOMAIN | | | | |
|---|---|---|---|---|
| | Frequency | Percent | valid percent | cumulative percent |
| STRONGLY AGREE | 42 | 42 | 42 | 42 |
| AGREE | 55 | 55 | 55 | 97 |
| STRONGLY DISAGREE | 1 | 1 | 1 | 98 |
| DISAGREE | 2 | 2 | 2 | 100 |
| TOTAL | 100 | 100 | 100 | |

Table# 03 Area functions to Domain level.

| ACCESS | | | | |
|---|---|---|---|---|
| | frequency | percent | valid percent | cumulative percent |
| STRONGLY AGREE | 42 | 42 | 42 | 42 |
| AGREE | 54 | 54 | 54 | 96 |
| STRONGLY DISAGREE | 4 | 4 | 4 | 100 |
| TOTAL | 100 | 100 | 100 | |

Table#04 IP range to manage access for users privilege.

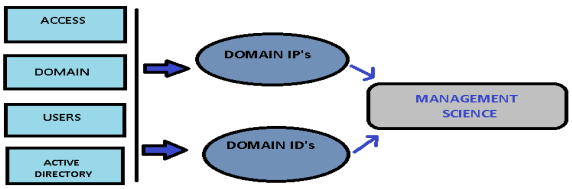
Testing IPV-4(TCP/IPV4) for Management IP setting frame to define sequence setting.




Fig# 02 Allows Gateway IP 192.168.1.1 / IP ADD range 192.168.1.1 – 50 DHCP Enabled when testing IPV-4(TCP/IPV4)

### 2.3 PROPOSED RESEARCH MODEL

This research method proposed model specification from workstation group to activate systems and security and to add administrative tools by Management. According to users privileges assigns users activity, roles, power authority, policies, users ID and IP Address.



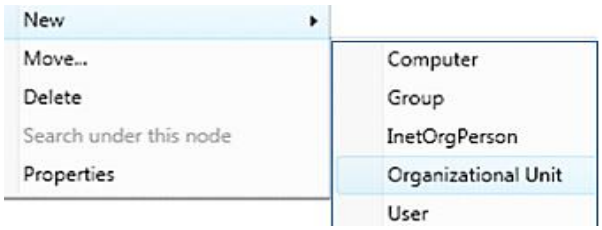

Fig# 03 shows proposed research method.

| MODEL SUMMARY | | | |
|---|---|---|---|
| Multiple Regression | R square | Adjusted R square | Apparent prediction Error |
| 0.7 | 0.491 | 0.446 | 0.509 |
| DEPENDENT VARIABLE: | MANAGEMENT | | |
| PREDICTORS: | ACCESS/DOMAIN/ACTIVE DIRECTORY/USERS | | |

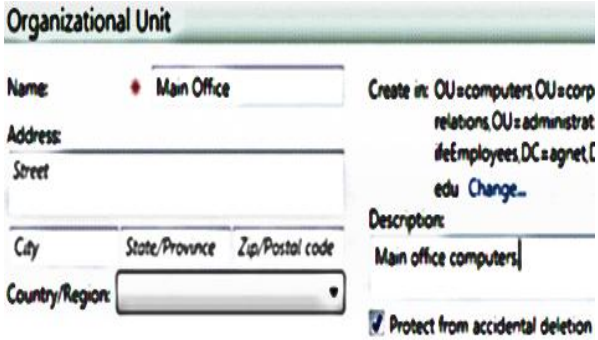
Table #05 Management is dependent upon its variables.

### 2.4 TREATMENT OF DATA:

Users privileges discusses to show how it treat with in more often to describes variables and assign activities to the user control access. This below data shows how to make groups and organizational units to assign privilege to user's work policy.




Fig# 04 contains OU that enables next system log-in permission.




Fig# 05 shows how to create Organizational Unit to assign further privilege.

### 2.5 SOURCES OF DATA

The sources of data in this research is being used is primary and secondary data both.

### 2.6 HYPOTHESIS

*$H_o$: Information Security ACCESS has a significant impact when Management.*

*$H_o$: DOMAIN IP's has a significant impact when Management.*

*$H_o$: ACTIVE DIRECTORY Admin have a significant role when Management.*

*$H_o$: USERS have a significant access when being controlled by Management.*

## 3. REVIEW OF RELATED LITERATURE & STUDIES

### 3.1 Cloud Identity & Access Management Model

Cloud IAM model is developed and tested with the experience research. The Cloud IAM model is a cloud based Identity & Access Management solution in both of a larger group and variety of organizations. In this research improve the model as cloud named and make it more scientifically in practice and develop new versions. The cloud IAM administrator gives full control to manage clouds digital rights and users access where, administrators can grant access to entire groups of users. Cloud user takes access through by airway while on sharing files or next system log-in to access via cloud ID. (Piepers Tim, 2013)[1]

### 3.2 Digital right management

The Digital Right management is created for the digital access to users who gets control on content consumer. E-books, databases and users of that information turn by libraries as content creators whom sources are directly present form digital right management. Digital right management focused on security and encryption as a mean of solving the issue and permissions over digital content. (puckett, 2010)[2]

### 3.3 The concept of role based access control

The concept stated from this research Role-based control is confidential part of users source management and it is associated with roles and users management with support of allowing users to assign roles permission, along with user role assignment that is what task would preferable with the goals designed in the form of departmental policies and roles, support groups of role relationships and constraints profiles that information is confidential part of user source of the research although may be significant difference on the software technique server manual security amplify through oracle or Sybase that allows multiple role for selection and information. (landwehr, 1995)[3]

### 3.4 The contradictory structures of system development methodologies

In this paper discusses the relationship between structures of system development methodologies may contain role of users and information system(IS) The science which being discuses on this research that the users are inconsistent and contradictory for their data emphasis on such about heavy loads and outcomes suggested recommended for partition between Enterprise source unit of the Central server and IT unit source which would become second backup if after any issue outcomes, backup will get save contradictory surface to units rely into must be secure. (Beath, 1994)[4]

### 3.5 Account management system

It is the control of computer systems allows various establishments of maintaining Roots accounts, client apparatus, derived account apparatus and throughout secure data that being derived from one system that save all data .TSM is an application who has vast

integration on storing capacity and records all financial and non-financial data. TSM (Tivoli storage management, IBM) is the Backup management which is the main source to make it centralized from networks support. (Ikeda, 2013)[5]

**3.6 E-Banking Management**

Automation is being vast inside knowledge now with secure granted log-in and log details by the users of workstation for them to communicate as they have all common data inside which will be secure from outside of the traffic which all being protected by firewalls. On the other hands E-Banking for outside traffic being programmed for the solution of advancement visibility information to customer view or marketing animation view. E-Banking is made with secure, convenient and reliable way to stay in touch with your account and take access to your account from anywhere after using web browser. It is ease of access and multiple option rights being visible on page for selection. (Clarke, 1950)[6]

**3.7 Role-Based Access control (RBAC): Features and Motivation**

In this research RBAC policies being described in terms user's management- operations and protected objects to operational control under RBAC when after creating active user in a role, the user must first being created for Domain ID after being authorized as a member of group role by security administrator. The subject of users role based management represents arrows from below relationships. Users <<---->> Roles <<---->> operations (Ferraiolo, 1992)[7]

**3.8 Web- Based Enterprise management architecture**

this research describes the management through architecture of Web-based Enterprise as a desktop management task forces as all data are common in the context of users activity model schema implemented by WBEM. The description of web-based Enterprise management discusses both substances itself. All systems being managed by standardized efforts. Some various communications being objected controlled by the Web-based Enterprise management including the object manager, providers, schema management and by network protocol administrators. (Thompson, 2002)[8]

**4. Data Analysis and results**

In this research we used regression model with simple regression and multiple regression to analyze with co-variant analysis to analyze continuous behavior of management which is dependent to the variable which being put to analyze how effective it would be through the data to construct from primary and secondary sources. Change in one variable (Management) predicts the changes to other variables. The regression method describes below

Test regression change in the prediction variable predicts the level of change in the outcome to present the dependent variable.

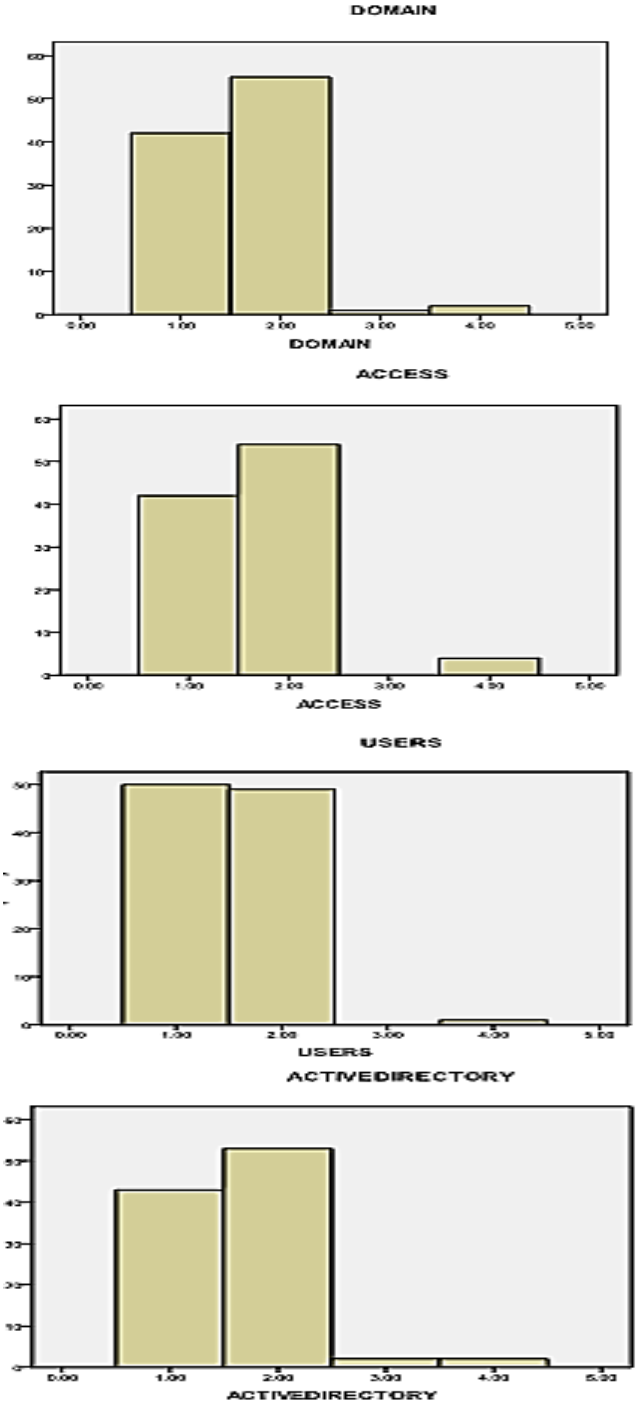
The combination of two or more variables predicts the level of change in the outcomes.

| | sum of squares | DF | mean square | Frequency | Sig. |
|---|---|---|---|---|---|
| Regression | 49.069 | 8 | 6.134 | 10.959 | 0 |
| Residual | 50.931 | 91 | 0.56 | | |
| Total | 100 | 99 | | | |
| MANAGEMENT | | | | | |
| Predictors: | ACCESS/ DOMAIN/ ACTIVE DIRECTORY/ USERS | | | | |

Table# 06 the combination of two or more variables predicts the level of change in the outcomes.

Above analysis is to test the standardized Coefficients on continuous dependent variables, controlling the effects variables. Below frequencies are conduct through based on Questionnaire sampling size100.

**Hypothesis:** Managemant has a significant impact on its variables.




**Graphs# 01 Positive result as Managemant has a significant impact on its variables.**

Chart# 01 Domain variable shows postive impact when management.

Chart# 02 Access variable shows postive impact when management.

Chart# 03 Users variable shows postive impact when management.

Chart# 04 Active directory variable shows postive impact when management.

**Acknowledgment:**
I would like to thank my parents was being with me till this stage of life and also thanks to my supervisor Dr. Asif Kamran. The door to research and excel my mind to work in the deparment of management sciences along with IT and Information Security knowledge and experiences to build secure management and knows very well there is further deep knowledge inside the field for creating advancement in corporate strategy.

**Conclusion:**

The purpose for this research is to give motivation along with the current active management strategy will get modified or penetrate with critical management and representing strategic management along with the strategy which centralized organizations are following. This research provides a framework for the implementation and maintenance of secure entity to centralized users which ensure confidentiality, availability and integrity of the systems management to control and monitor the risk from unnecessary threats and data loss by accidental or intentional modification, disclosure or destruction. Domain policy will all applies from one central root to manage user's entity and mitigate organizations exposure to systems risk.

**Recommendation:**
Advantage from this research is that, system administrators are provided access by statically and define roles, hierarchies, relationship departmental policies by the principal administrative actions performed when required and through process updated, granted access and revoke users from assigned temporary roles for temporary time. object Role activation with above active subject is through mapping of user's application from software settings, where port number, license, user role, IP being set up to the application inside settings as to perform roles according to policy consideration taken into account that pertain users to perform task or operation after users organization's work project.

**REFERENCES:**

1. Beath, C. M. (1994). The Contradictory Structures of System Development Methodologies. Moodle.
2. Clarke, S. (1950). E-Banking Management. http://www.igi-global.com/reference.
3. Ferraiolo, D. F. (1992). Role-Based Access Control(RBAC). U.S Department of commerce Gaithersburg MD 20899.
4. Hartung, F. (2002). Digital Rights Management and Water marking of multimedia content for M-commerce Applications. IEEE communications magazine, 2000 - ieeexplore.ieee.org.
5. Ikeda. (2013). Account Management System- root account management, apparatus, derived account and program. United states Patient Documents, US patent No. US8499147B2.
6. landwehr, C. (1995). The concept of Role-Based Access Control(RBAC). IEEE Computer, volume 29, number 2, february 1996,, pages 38-47.
7. Piepers Tim. (2013). Cloud identity & Access Management Model. International journal of Management Sciences & Computer Science, Springer
8. puckett, J. (2010). Digital rights management as information access barrier. progressive librarian, 34/35 International journal, http://www.progressivelibrariansguild.org/PL_Jnl/pdf/PL34_35_fallwinter2010.pdf, 11-24.
9. Ramaswamy, C. (1994). Commercial Database Management System. *computer security division, ITL NIST, Gaithersburg, maryland 20899 chandramouli@csmes.ncsl.nist.gov*.
10. Thompson, J. (2002). Web-base Enterprise Management Architecture. *IEEE Communications Magazine, volume 36, DOI: 10.1109/35.663331* , Issue 3.

About Author (s):