International Journal of
Computing, Programming and
Database Management

Nalabothu Sravanthi
M. Tech Student, IV Semester,
Visvodaya Engineering
College, Kavali, Andhra
Pradesh, India

Dr. B Konda Reddy
Professor, Department of
Computer Science and
Engineering, Visvodaya
Engineering College, Kavali,
Andhra Pradesh, India

Microsoft Ad & azure SSO integration with ServiceNow

Nalabothu Sravanthi and Dr. B Konda Reddy

Abstract
Service Now is an application-platform-as-a-service provider, providing technical management support, such as IT service management, to the IT operations of large corporations including Service Portal for customers and employees. Service Now provides user management with groups and role management out of the box. In large corporations it is very difficult to manage the users and access control for individual applications. To overcome these setbacks integrating the application with Active Directory is the one simple and widely used solution. Microsoft's Active Directory (AD) is a directory service used to store information about network resources across and provides a hierarchal way to the entire network of users, devices and applications. Active directory stores information about network resources such as users, user's password, groups, network printer and computer and make the information available to users and administration. Microsoft introduced Azure AD, a cloud-based PaaS service in its Azure suite, which offers Single Sign on (SSO) along with AD. In this thesis, integrating these two tools with ServiceNow for seamless User and Access management along with SSO.

Keywords: ServiceNow, microsoft AD, Azure SSO, ServiceNow AD integration -x-

Introduction
Application platform as a service (aPaaS) is a cloud service that offers development and deployment environments for application services. ServiceNow is a cloud-based application that provides application platform as a service (aPaaS) for IT services management (ITSM), IT operations management (ITOM) and IT business management (ITBM), IT Asset Management (ITAM), allowing users to manage projects, teams and customer interactions. ServiceNow can integrate with other tools easily. For example, Microsoft Active Directory, MS Teams, Slack, Salesforce and other tools which offer API. In the current scenario, for user management and controlling access to different applications in enterprise network Active Directory is the way. Otherwise managing users at application level is herculean task. And at the same time, for end users it is difficult to memorize the passwords for various applications they interact with in their day-to-day work. To simplify this, organizations are implementing Single Sign On authentication (SSO) for access control, SSO provides seamless access to applications with minimal and secure authorization protocols. Azure SSO introduced by Microsoft as part of its Office 365 suite is the trend these days.

Objective
The main objective of this project is integrating Microsoft AD and Azure SSO with ServiceNow for user management and access control. In the current scenario, the organization doesn't have LDAP for achieving this requirement. This work aims at achieving the organization's requirement using customized MS AD Spoke and RESTAPI.

Literature survey
Cloud computing
Cloud technology is a model for providing convenient network access mode "on demand" to common computing resources, for instance: applications, services, networks, servers, database storages, etc. There are several cloud services models:
▪ Software as a Service (SaaS)
▪ Platform as a Service (PaaS)
▪ Cloud Infrastructure as a Service (IaaS)

Corresponding Author:
Nalabothu Sravanthi
M. Tech Student, IV Semester,
Visvodaya Engineering
College, Kavali, Andhra
Pradesh, India

Servicenow

ServiceNow - is a company providing cloud service, SaaS for enterprises and organizations.

ServiceNow is focused on transformation of information technologies by automating and standardizing business processes, as well as their integration across the enterprise.

According to analysts, ServiceNow is a leader in the field of ITSM-making (IT Service Management). The company offers a unified cloud platform for the automation of the life cycle for IT-services, project management, personnel, resources, risks, etc. (Figure 2.1).

Fig 1: Service Automation Platform

The most interesting features of the system include:

- Strict separation of platform layer and application layer, which allows you to migrate to a new version of platform in a few hours
- Well-developed visualization tools
- Content management that allows to create complex portals for users
- Ability to create applications by users (there is a portal share.servicenow.com, where users can publish their own applications and share them)
- Wide availability of process and technical documentation on the system - support.servicenow.com

Service Management

ServiceNow changes the way people are working. It is oriented on the activities, tasks and processes that we meet in everyday life. ServiceNow enables you to focus on creating a modern work environment. The module of ServiceNow is built in the way that all work is atomized, including email deleting and spreadsheets, optimizing the delivery and managing services.

Common service model – is effective service management. It is provided for the customers of ServiceNow to have standardized enterprise service management, which is applied to many different areas in and out of IT, such as HR, facilities, field service and other service domains that are used for service relationship management (Figure 2.2).

Fig 2: Service relationship model

Custom application development

Complexity, slowness and expense cost of developing software grow every day. It is related to business problems that enterprise owners meet. So, for certain issues customers need customs solutions and applications to deal with those issues. ServiceNow has good decision to help with different kinds of needs, it is App Studio Development Suite. With the help of this tool users are available to create different applications for separate departments or even whole enterprise.

Business management

There are several advantages that could be reached to the enterprise. For instance, Business Management improves perceptibility and users are able to guide the most valuable assets such as labour, projects and merchants. Data developing is useful for defining costs, resource usage, management project automation, business relations, etc. In reverse of trusting to diverse software like spreadsheets and electronic mail, user can allow the project teams for better and faster work, merchants to advance their work and decrease the tariff, as well as cut down the influence of risk and simplify the work process by automation.

IT operations management

All customers are waiting for a new business service, but the limited functionalities and dependencies in the service could create some issues and as a result you will not get exactly that you were expecting.

ServiceNow service automation platform

ServiceNow service automation platform is a solution for the automation of IT services. ServiceNow platform enables applications adapting and developing service delivery models in the automation of both IT and other business processes of the enterprise. There are lot of key features of portal that help customer to manage processes. First of all, it is the ability to self- configure user's form, so a user can add or remove some fields and change other form setting. Then, easily creation and grouping any information in the system into reports. Graphic editor for development process of any system objects. One of the most useful functions are chat, news and discussions modules. In addition, a customer gets access from any mobile device without special software. And the last one - the ability to develop your own applications and portals without programming.

Mid server

Management, Instrumentation, and Discovery (MID) server is a Java application that runs on a server on your local network. MID Servers facilitate communication and data movement between a single ServiceNow® instance and external applications, data sources, and services.

MID Servers help you to control and secure how ServiceNow communicates with your organization's systems, especially those behind a firewall. This supports four primary use cases:

1. Integrations: Supporting LDAP, JDBC, REST, and SOAP based integrations to systems on intranet.
2. Orchestration: Enabling orchestration with other systems via either workflow activities or Integration Hub spokes

3. Discovery: Providing access to systems for traditional CI discovery and / or to support discovery needed for service mapping
4. Attach Script File: MID Server Script Files can be used to communicate with targeted devices (e.g., PowerShell, JavaScript, bat)

Integration hub

Integration Hub enables execution of third-party APIs as a part of a flow when a specific event occurs in ServiceNow. These integrations, referred to as spokes, are easy to configure and enable you to quickly add powerful actions without the need to write a script. For example, you can post a message and incident details in a Slack channel when a high priority incident is created.

Microsoft AD

Active Directory (AD) is a directory service developed by Microsoft for Windows domain networks. It is included in most Windows Server operating systems as a set of processes and services. Initially, Active Directory was used only for centralized domain management. However, Active Directory eventually became an umbrella title for a broad range of directory-based identity-related services.

Azure SSO

Single sign-on is an authentication method that allows users to sign in using one set of credentials to multiple independent software systems. Using SSO means a user doesn't have to sign into every application they use. With SSO, users can access all needed applications without being required to authenticate using different credentials. For a brief introduction, see Azure Active Directory single sign-on. Many applications already exist in Azure AD that you can use with SSO. You have several options for SSO depending on the needs of the application and how it is implemented. The management of applications can be made easier by using the My Apps portal.

Implementation plan

For this work the implementation is divided into two parts, 1. AD Integration and 2. Azure SSO integration. For this, A Windows Server 2019 is configured in a VM which acts host for AD and MID Server. So ServiceNow can connect to the AD through the MID Server. For Azure SSO implementation, an azure subscription is taken with Pay-As-Go pricing, which offers free AD up to 50,000 users.

Implementation- ad integration

The project experimental setup desires operating system Windows Server 2019, MID Server, Active Directory, ServiceNow Instance and Azure Subscription.

ServiceNow instance

ServiceNow offers free instance for developers, for this work a PDI is requested from ServiceNow from https://developer.servicenow.com.

Active directory configuration

1. Open Server Manager - Hit "Windows" key on your keyboard and type "Server Manager" to search for the application. Once it is open as illustrated by the figure below, let us now proceed to the next step of installing Active Directory Domain Services.

2. Add Roles and Features - Right- click on "Manage" on the "Server Manager" window and choose "Add Roles and Features". This will open the "Add Roles and Features Wizard" which ushers us to the part where we install Active Directory Domain Services. Click on next.
3. Installation Type - On the "Installation Type", leave "Role- based or feature-based installation" radio button selected and click on next.
4. Server Selection - On this stage titled "Select destination server", select the server you are to install AD DS and click next. I am going to choose my local server.
5. Server Roles - The previous step will lead you to the next page as shown below. Here, you will see many options with square checklist box against them. As you can guess, we are going to choose "Active Directory Domain Services".
6. Add Features - Immediately you choose that option, a new part comes up. On the page, just click on "Add Features" tab and hit "Next".
7. Select Features - On the next page after Step 6 titled "Select features", just hit "Next" to lead you to installations of AD DS.
8. AD DS - As shown below, you will be presented with the next page titled "Active Directory Domain Services". Here, click on "Next"
9. Confirm your selections - The next page is about confirming what you need to install before actually installing them. If you are sure about what you have chosen, click on install. You can optionally choose the option that restarts the server whenever required. Click on close once it is done.
10. Promote to Domain Controller - After you have finished installing Active Directory Domain Services, the last step is to promote it to a Domain Controller. Go over to Server Manager where you will notice a yellow exclamation notification beside the "Manage" tab as shown below. Click on it and choose "Promote this server to a domain controller"
11. Add a new Forest - A new window titled "Active Directory Domain Services Configuration Wizard" as shown below will pop up. We are going to add a new Forest but in case you would wish to do something different in this Step, you are free to choose the other options. Add your organization's root domain name. Click on "Next" after you pick your choice.
12. Domain Controller Options - On the Domain Controller options, leave the defaults checked and input your password. After that, click "Next".
13. DNS Options - On the next page (DNS Options), you will probably see an error on top with the words "A delegation for this DNS server cannot be created because the authoritative parent zone name server cannot be found". Ignore it and click "Next"
14. NetBIOS domain name - On the next page, leave the NetBIOS domain name as default or you can change it as long as it is not longer than 15 characters. Click "Next" after that.
15. Paths - Leave paths as default and click "Next" as shown below.
16. Review Selections - In this step, the server allows you to review what you have done so far. If you are good with the selections you have done. Hit "Next".

17. Prerequisites Check - In this step prerequisites will be validated before Active Directory Domain Services is installed. If you get any errors here, please look at it and fix anything in the previous steps. If all is okay, click "Install".
18. After that, the Server will reboot and you can then log into the Domain with the credentials you set in Step XII.

Installation and configuration of mid server

MID server is configured using guided setup and validated the MID Server after configuration.

Fig 3: Validated MID Server

Install integration hub & Microsoft ad spoke

1. Navigate to https://developer.servicenow.com and login with credentials.
2. Click on Profile and select **Activate Plugin** in My Instance section.
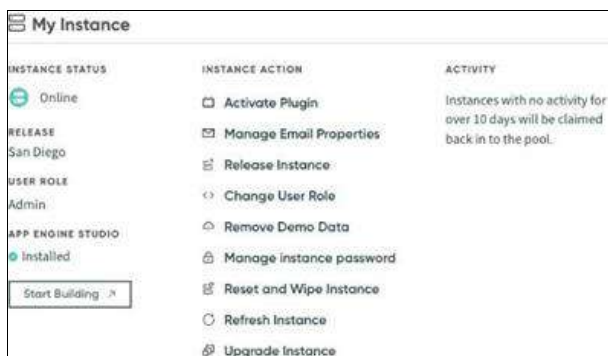

Fig 4: My Instance Screen

Search for Integration Hub and **select "ServiceNow Integration Hub Enterprise Pack Installer"** and click on Activate.
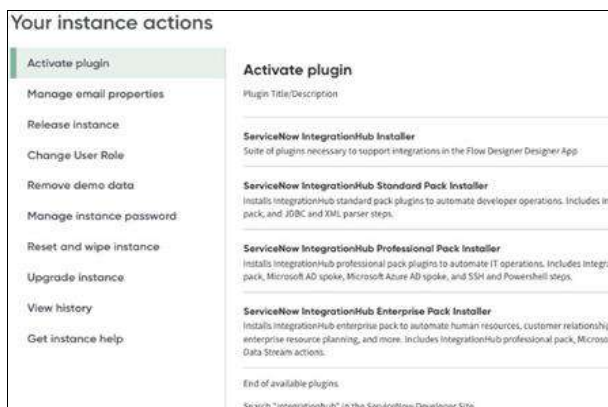

Fig 5: Plugin Installer Screen

Once the plugin is activated, open PDI and navigate to System Definition > Plugins and search for "Microsoft AD Spoke for Integration Hub" and install.
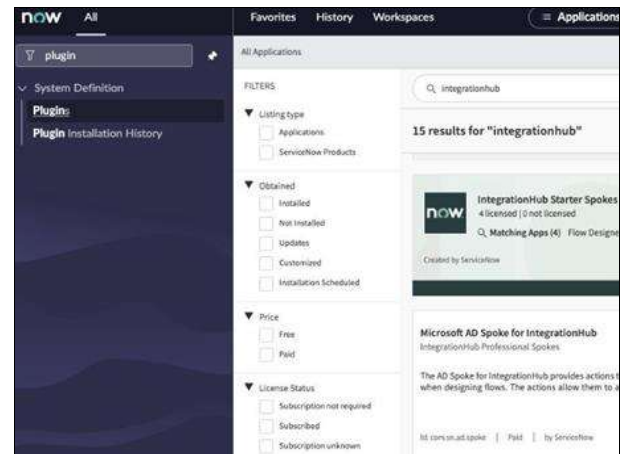

Fig 6: Plugins page in SNOW Instance

Configure Microsoft AD spoke

Create a Credential record for the Microsoft Active Directory host. The Microsoft AD spoke connection and credential alias uses this credential to authorize actions.

Create a Connection record to your Microsoft Active Directory host machine. The Microsoft AD spoke connection and credential alias uses this connection to perform actions in Microsoft Active Directory.

Develop custom ad spoke action

The Out of the Box AD Spoke doesn't contain the Action for retrieving the users in bulk and sync them with ServiceNow user table. To achieve this a custom Action is designed which parses the JSON object of users retrieved from AD using Query AD action and process the user data and populate the user details like,

a) First name
b) Last name
c) Email
d) Title
e) Mobile
f) **Department:** This value is stored in cmn department table and references the record to the user in sys user table.
g) **Company:** This value will be referenced from core company table.
h) **Location:** This field is populated from the cmn location table, the cmn location table is populated from the Street, City, State, Country and ZIP fields.
i) **Manager:** The manager field is populated same sys user table, if the manager is found in the sys user table he sys id will be used for reference otherwise a new user will be created and referenced.
j) **Groups:** The user will be added to the groups which he is part of.

Custom flow for user and group syncing

ServiceNow provides Flow designer for process automation. Flows are used to automate repeated tasks such as approvals, data transformation etc. Here, a custom flow is developed which retrieves the users from AD using the Query AD action and Custom flow "Process AD JSON".

Testing
Navigate to the custom Flow Process Automation > Flow Designer > Flows > "Sync AD Users" and click on the button Test. This will run flow instantaneously and this should fetch the users from AD and the user records should be available in sys user table.
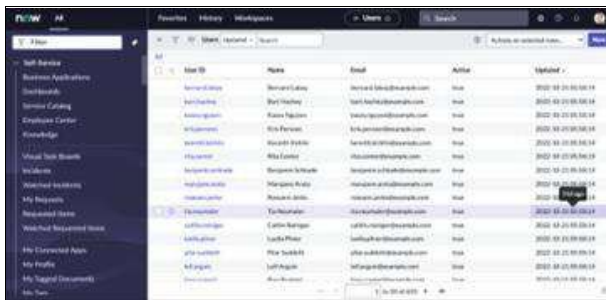
Fig 7: User records in sys user table

Implementation-azure SSO
The project experimental setup desires Azure Subscription and ServiceNow instance with "Integration-Multiple Provider Single Sign-On Enhanced UI" plugin enabled.

Install integration multi procider SSO plugin
1. Navigate to https://developer.servicenow.com and login with credentials.
2. Navigate to System Definition > Plugins and search for "Integration - Multiple Provider Single Sign-On Enhanced UI" and install.
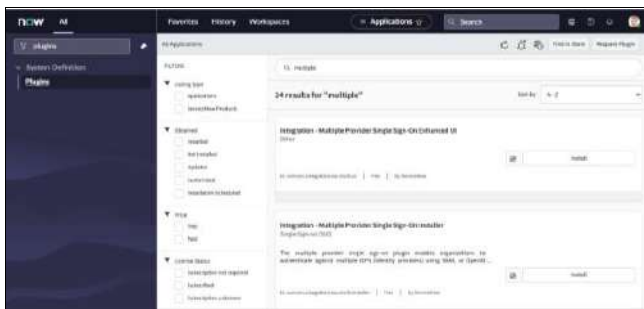
Fig 8: Plugins page in SNOW Instance

Configure azure ad SSO for ServiceNow
Add ServiceNow from the gallery
To configure the integration of ServiceNow into Azure AD, you need to add ServiceNow from the gallery to your list of managed SaaS apps.
a) Sign in to the Azure portal by using either a work or school account, or by using a personal Microsoft account.
b) In the left pane, select the Azure Active Directory service.
c) Go to Enterprise Applications, and select All Applications.
d) To add new application, select new application.
e) In the Add from the gallery section, enter ServiceNow in the search box.
f) Select ServiceNow from results panel, and then add the app. Wait a few seconds while the app is added to your tenant.

Configure Azure AD SSO
a) In the Azure portal, on the ServiceNow application integration page, find the Manage section. Select single sign-on.

b) On the Select a single sign-on method page, select SAML.
c) On the Set up single sign-on with SAML page, select the pen icon for Basic SAML Configuration to edit the settings.
d) In the Basic SAML Configuration section, perform the following steps:
e) In Sign on URL, enter https://dev61370.service-now.om/ navpage.do
f) In Identifier (Entity ID), enter a URL that uses the following pattern: https://dev61370.service-now.com For Reply URL, https://dev61370.service-now.com./navpage.do In Logout URL, enter https://dev61370.service- now.com./navpage.do
g) Select the copy button to copy App Federation Metadata Url, and paste it into Notepad. This URL will be used later in ServiceNow instance.
h) In the Set up ServiceNow section, copy the appropriate URLs, based on your requirement.

Create an Azure AD test user
1. From the left pane in the Azure portal, select Azure Active Directory > Users > All users.
2. Select new user at the top of the screen.
3. In the User properties, follow these steps:
4. For Name, enter Sravanthi Nalabothu. For User name, enter the sravanthi @ thegeekconsole.com
5. Select Show password, and then write down the value that's shown in the Password box.
6. Select Create.

Assign the Azure AD test user
1. In the Azure portal, select Enterprise Applications > All applications.
2. In the applications list, select ServiceNow.
3. In the app's overview page, find the Manage section, and select Users and groups.
4. Select Add user. In the Add Assignment dialog box, select Users and groups.
5. In the Users and groups dialog box, select Sravanthi Nalabothu from the users list, and then choose Select.
6. If you are expecting a role to be assigned to the users, you can select it from the Select a role dropdown. If no role has been set up for this app, you see "Default Access" role selected.
7. In the Add Assignment dialog box, select Assign.

Configure ServiceNow
1. Sign on to your ServiceNow application as an administrator.
2. In the left pane, search for the Multi-Provider SSO section from the search bar, and then select Properties in the Administration.
3. In the Multiple Provider SSO Properties dialog box, perform the following steps:
▪ For enable multiple provider SSO, select yes.
▪ For Enable Auto Importing of users from all identity providers into the user table, select yes.
▪ For Enable debug logging for the multiple provider SSO integration, select yes.
▪ For The field on the user table that. enter email.
▪ Select Save.

You can configure ServiceNow automatically or manually. To configure ServiceNow automatically, follow these steps: Return to the ServiceNow single sign- on page in the Azure portal.

One-click configure service is provided for ServiceNow. To enable this service, go to the ServiceNow Configuration section, and select Configure ServiceNow to open the Configure sign-on window.

In the Configure sign-on form, enter your ServiceNow instance name, admin username, and admin password. Select Configure Now. The admin username provided must have the security-admin role assigned in ServiceNow for this to work. Otherwise, to manually configure ServiceNow to use Azure AD as a SAML Identity Provider, select manually configure single sign-on. Copy the Sign-Out URL, SAML Entity ID, and SAML single sign-on Service URL from the Quick Reference section.

Sign on to your ServiceNow application as an administrator. In the automatic configuration, all the necessary settings are configured on the ServiceNow side, but the X.509 Certificate isn't enabled by default and give the Single Sign-On Script value as MultiSSOv2_SAML2_custom.

You have to map it manually to your identity provider in ServiceNow. Follow these steps:

In the left pane, search for the Multi-Provider SSO section from the search box, and select Identity Providers.

Select the automatically generated identity provider.

On the Identity Provider section, perform the following steps:

1. Right click on the grey bar at the top of the screen and click Copy sys id and use this value to the Sign on URL in Basic SAML Configuration section.
2. For Name, enter a name for your configuration (for example, Microsoft Azure Federated single sign-on).
3. Copy the ServiceNow Homepage value, and paste it in Sign- on URL in the ServiceNow Basic SAML Configuration section of the Azure portal.
4. Copy the Entity ID / Issuer value, and paste it in Identifier in the ServiceNow Basic SAML Configuration section of the Azure portal.
5. Confirm that Name ID Policy is set to urn: oasis: names: tc: SAM L:1.1:nameid- format: unspecified value.
6. Click on Advanced and give the Single Sign-On Script value as MultiSSOv2_SAM L2_custom.
7. Select Save.
8. At the upper-right corner of the page, select Test Connection.
9. When asked for your credentials, enter them. You'll see the following page. The SSO Logout Test Results error is expected. Ignore the error and select Activate.

ServiceNow test user

Create a user called Sravanthi Nalabothu in ServiceNow with the same email as given in Azure AD user creation.

Test login

Open the ServiceNow instance https://dev61370.service-now.com, it should redirect to Microsoft Azure SSO Login page instead of conventional ServiceNow login page. Try logging in with username sravanthi@thegeekconsole.com, after successful authentication, it will be redirected to SNOW home page.

Conclusion

The objectives of this project are achieved successfully. The following conclusions are drawn from this work.

Microsoft AD can be integrated with ServiceNow for user synchronization without using LDAP and transform maps.

Custom Actions can be developed in ServiceNow with which the OOB Spokes can be extended to achieve the custom requirements.

SSO is configured with Azure, which enabled the seamless login process with minimal authentication steps, when the user is connected to enterprise network.

Access management can be handled through AD itself using the groups. The users in AD group can be added to the respective ServiceNow group.

User management became easy and overhead on SNOW Admins is reduced from user management active.

References
1. Directory System Agent. MSDN Library. Microsoft. Retrieved; c2014. Apr 23.
2. Solomon, David A. Russinovich, Mark. Chapter 13. Microsoft Windows Internals: Microsoft Windows Server 2003, Windows XP, and Windows 2000 (4th Ed.). Redmond, Washington: Microsoft Press; c2005 p. 840. ISBN 0- 7356-1917-4.
3. Hynes, Byron (November 2006). The Future of Windows: Directory Services in Windows Server Longhorn. TechNet Magazine. Microsoft. Archived from the original on 30 April 2020. Retrieved 30 April 2020.
4. Active Directory on a Windows Server 2003 Network". Active Directory Collection. Microsoft. 13 March 2003. Archived from the original on 30 April 2020. Retrieved 25 December 2010.
5. Rackspace Support (27 April 2016). Install Active Directory Domain Services on Windows Server 2008 R2 Enterprise 64-bit. Rackspace. Rackspace US, Inc. Archived from the original on 30 April 2020. Retrieved 22 September 2016.
6. HabrHabr. 1000 words about the future of cloud technologies. URL: http://habrahabr.ru/company/ua-hosting/blog/239131/.
7. HabrHabr. ITIL for developers. URL: http://habrahabr.ru/company/dataar t/blog/237263/.
8. Helios Information Technologies. ServiceNow – a fresh eye for IT management. URL: http://hbc.ru/services/optimizacia/servicenow/.
9. Kontur. Business on the cloud. What are the advantages of cloud technologies for entrepreneur? URL: https://kontur.ru/articles/225.
10. MWT Solutions. ServiceNow. URL: http://mwtsolutions.pl/servicenow/r u/index.html.
11. ServiceNow. Business
12. Management. URL: http://www.servicenow.com/soluti ons/ business-management.html.
13. ServiceNow. Custom Application Development. URL: http://www.servicenow.com/soluti ons/application-development.html.
14. ServiceNow. IT Operations Management. URL: http://www.servicenow.com/solutions/itoperations-anagement.html.
15. ServiceNow. Products and Solutions. URL:http://www.servicenow.com/products/productsby-category.html.
16. ServiceNow. Service Management. URL:http://www.servicenow.com/s olutions/servicemanagement.html.
17. ServiceNow wiki. Case study – Building Our Website in CMS. URL:http://wiki.servicenow.com/in dex.php?title=Tutorial Building_ Our Website in CMS