AM-2 NIE API Gateway in NIE

Who uses the APIs now and how is the adoption rate?

The APIs are used by our faculty, our corporate mobile app users, corporate systems and students, the adoption rate is growing healthy at a steady rate. We are moving away from data level integration to api level integration.

Which EA framework NIE used and who drives it?

It is largely based on TOGAF there was a team with enterprise architect and technical architect driving the first version.

What are the limits on API use?

So far, we have not put bandwidth or usage limits on the APIs.

How do you resolve latency issue on multiple API call on 1 front end action?

The latency is not much and if performance is an issue especially for a meshed-up api (via orchestration), we may implement caching for readonly type of APIs.

How do you manage life cycle of an API?

The API has to be documented and on boarded in an orderly manner. We have an onboarding process to full test and document the API before it is published to production server.

What are the challenges on API journey?

2 main challenges: mainly the people mind-set change and selection of the appropriate product applied.

Does the CA API GW comes as a hardware appliance?

No, it either comes as a software package or a virtual appliance.

How many backend systems have you integrated?

More than 15 backsystems, ranging from corporate on premises systems, corporate SAAS (Workday, ServiceNow – done with our NTU colleagues), academic systems and teaching and learning systems.

How often do you kill off API?

No far none.

How do u monitor api usage and hence housekeep to avoid resources hogging?

We monitor using the logs on the CA API gateway.

Any changes to be made at target systems?

Yes mainly for bespoke systems, there has to be a web services or integration layer to be introduced to wrap around already well defined services.

Is there any major client using this API services?

The APIs are used by our faculty, our corporate mobile app users, corporate systems and students, now we are co-creating apis with our NTU colleagues because of shared systems such as WorkDay and ServiceNow.

How do you handle large payload?

By introducing throttling policies and size restriction for multimedia uploads.

What has been done to ensure high availability since all requests from client to backend goes via API gateway?

Basically firewall rules are only opened from system to api gateway and not system to system.

How is the security put in place?

API keys, SSL verification or server IP whitelisting depend on whether is it client to server or server to server type of api.

How many APIs have you developed in your 2 years journey?

20 to 30 and growing.

On security, how do you authenticate and authorize front end?

Please see response to above question on security.

What are the pain points that you face when using microservices?

Not much pain point but I would think that adoption could be accelerated by enhancing the support for underlying application infrastructure and influencing people’s mind-set. Micro services require the pervasive use of API gateways and/or queue mechanisms and this works better when implemented under a cloud stack supported by application containerization technologies such as Docker. For a on premise implementation, the natural way is implement in a monolithic design as most system objective are driven by “silo” type of business requirements rather than from a holistic enterprise architecture type of scope.

The second point is perhaps changing people’s mind-set to encourage system designers to find opportunities of streamlining and design in a holistic manner rather than a standalone, clearly drawn boundary.

AM-3 NIE Federated-SSO for Cloud Applications

1. Do u have sso to in house enterprise application? Handle their roles and what they can access?

Ans: Yes, we have implemented Web-SSO for In-house Enterprise applications.

Yes, we are using Access Matrix for Access Control Management and Authorization. The application specific authorization information is stored in database tables.

2. Azure AD supports SAML. Any use of it?

Ans: Yes, Azure AD provides Active Directory Federation Services using SAML. We are exploring on this product for comparison purpose.

3. Do you use Azure AD?

Ans: NO. We are using Access Matrix (solution) from i-sprint for federated-sso.

4. What are the products used for the SSO?

Ans: i-sprint Access Matrix - Universal Single Sign-on.

5. How is security ensured?

Ans:

To make it secure, we can digitally sign the response with our private key and share the certificate with the Service provider. In this way it can provide the security against fake IdP and "Man in the middle" attack (MITM).

Apart from that, it is always recommended to have this transaction to be HTTP over SSL.

The SAML specifications recommend, and in some cases mandate, a variety of security mechanisms:

- TLS 1.0+ for transport-level security
- XML Signature and XML Encryption for message-level security

6. How to make the look and feel of the common login module to look the same as the service provider

Ans: There will be only one login page provided by the Identity Provider, as the authentication is provided by the identity provider (IDP).

7. How large is NIE access management team?

Ans: Two headcounts

8. What product are you using?

Ans: Refer question 4.

9. Does IDP store all user access roles from each service providers?

Ans: The Service provider does not provide any ACL to store in IDP. Instead, the Service provider takes the ACL given by the IDP. The ACL is created and maintained by the IDP and send over to service provider.

10. How is the IDP & API working together in the big picture?

Ans: For some service providers, the SAML integration works via SOAP or REST API's. In order to manage or consume API's, we will be using NIE API gateway.

11. How large IA your user base?

Ans: 6000 users (Approximately 5000 NIE Students + 1000 NIE Staff)

12. How do you handle external users? (non nie)

Ans: We are using local domain feature in Access Matrix to manage/handle external users. For example we have created "vendors" local domain in AM.

13. Since sso only requires single factor authentication (i.e AD), is the team looking at MFA solution?

Ans: Yes, we are exploring on Multi Factor Authentication. Soft Token Base.

14. How does sso on encryption use?

Ans:

To make it secure, we can digitally sign the response with our private key and share the certificate with the Service provider. In this way it can provide the security against fake IdP and "Man in the middle" attack (MITM).

Apart from that, it is always recommended to have this transaction to be HTTP over SSL.

15. What if SP does not support SAML?

Ans : We can use other protocols like oAuth or OpenID Connect.

16. How does sso on cloud integration with block chain for education net?

Ans: We are still on an exploration stage on SSO for block chain. In fact Block Chain is emerging as a secure authentication provider. I would like to share an interesting article on ***"Application of the Blockchain for Authentication and Verification of Identity"*** from Ben Cresitello-Dittmar.

http://www.cs.tufts.edu/comp/116/archive/fall2016/bcresitellodittmar.pdf

17. How do you prevent man-in-middle attack, where someone steal your token and goes into your entire ecosystem impersonating you?

Ans: Refer question 5.

18. How long it takes to implement by adding one additional service provider?

Ans: Only setting up the IDP platform takes time. Once the Identity Provider (IDP) setup is ready, additional service providers can be configured within one or two days provided the service provider support SAML and have full technical knowledge.

19. How to interface with block chain?

Ans: Refer question 16.

PM-Track1-2 SUTD Asset management system - end to end complete workflow

Is the asset lifecycle being managed and automated in AMS?

SUTD: Yes

Do you have a business process re-engineering unit to redesign the processes and workflow?

SUTD: No. The business unit in-charge of the requirements is the Office of Finance

Was it easy to setup approval workflow in AMS?

SUTD: Yes because the platform is workflow driven but we left it to the vendor to configure the workflow

How would you handle certain exceptions, due to slowness in updating of data from upstream systems? E.g. Schools forget to update staff departure dates?

SUTD: Finance is responsible for such data update and they are also the final approving party for exit clearance. In the event if there is gap in such data update, Finance can immediately initiate an exit clearance workflow

What AMS are you using? Off the shelf or customised?

SUTD: Off the shelf with customisations

Does ams also capture the maintenance contract for some of the applicable assets? And if yes, does the sys facilitate auto email notifications when contract is due for renewal?

SUTD: Nope.. This is not handled in the scope. We are going to have another system for it

Was it a Big Bang implementation?

SUTD: Nope… we had 2 phases. 1st phase was just asset record management and verification but the 2nd phase was of a much bigger scope with the asset lifecycle

Are you part of IT or Finance department ?

SUTD: We are from IT.

What is the frequency used by the RFID?

SUTD: 920-925 MHz, ultrahigh frequency; 13.56 MHz high frequency

How long does it take to implement?

SUTD: All in all, about 9 months but we had a gap of about 2 months due to peak period

Do u still need to use scanner or can use mobile phone to scan?

SUTD: The scanning of asset tags during asset verification is by iPhone or iPad only but you can normal scanner to read in the QR code to facilitate data entry

How much does the AMS costs?

SUTD: Implementation plus 1 year maintenance was about S$136K

What software are you using for AMS?

SUTD: MS SQL Database 2012, .Net application with C-Sharp

Is the AMS a bespoke or COTS application?

SUTD: COTS

PM-Track1-3 NIE Student Forms Automation in NIE

Is there any alignment of such digital forms with NTU ?

Not yet, so far the forms are all from NIE and dealing with academic matters for NIE students.

Can you dynamically include one form fast ?

Yes for forms that are built on Outsystems yes (1 to 2 days) but for .NET forms it will take 2 to 3 days.

How do you handle forms that are court admissible?

We will link it as a pdf form to be printable manually. (Especially insurance forms that requires signature)

How long did u take to implement?

For completion of digitalization its 10 months, for total automation of workflow, it will take approximately 1.5 years.

How many in the team currently?

1 Project manager, 1 business analyst, 1 technical architect, 1 analyst programmer and a team of outsource developers (typically 1 to 3 developers).

Is this in-house development?

Yes, it is considered an-house development despite us having outsource developers. However no one size fits all, some IHL may consider to use SAAS such as ServiceNow forms or Office365.

Are these forms digitised or digitalised? If it's the latter, which system stores all these information ?

It is a bit of both, some forms are digitised first and that enables windows of opportunities to open up more value added services. Others are digitalised meaning we align both business and technology side to ensure that students leverage off the most value off our online services. That is why the head of a digitalisation project is typically a power business user. In NIE's case, it is our Deputy Director of Admission Office who heads the implementation committee. He helps to manage and streamline the project across offices, balancing technological and technical concerns.

The information is stored our student lifecycle system (ISAAC) as json format in Oracle RDMS (similar to NOSQL concept)

What software did u use for your workflow engine?

We have not identified our workflow engine but it is likely to be built around an .NET workflow component since our approach was to enhance our students system to handle the digital forms.

How were the urls stored in the oracle used?

It is stored as urls in table format pointing to links in Oracle directory.

PM-Track1-4 SMU Chatbot for Student Services: A Case Study for Singapore Management University

Is the Data Governance Module of SAS important or essential in any Analytics project?

Thanks, I don't think this is a question for this session ;P

What are the main differentiators between IBM Watson and Microsoft Cognitive Services?

Our experience is limited to the IBM Watson Assistant (formerly Watson Conversation) part of the IBM Cloud, so it may not be a comprehensive comparison. Both platforms have broad set of services, and are generally rich in documentation for developers. There is a QnA maker service in Microsoft that is easy for getting started with FAQs. We feel IBM Watson Assistant has a deep machine learning capability which is well established. Perhaps the link below gives a fuller comparison

https://marionoioso.com/2017/03/15/ibm-watson-services-vs-microsoft-cognitive-services-1/

Great presentation. Thank you.

Thanks!

How much to implement Watson?

In the Watson Assistant Pay-as-u-go Standard tier cloud subscription, you have

- Unlimited API queries per month
- Up to 20 Workspaces
- Up to 2000 Intents
- Up to 1000 Entities
- Shared Public Cloud
- *POST /message method calls only

The current rate is USD25 for 10,000 API calls. You get USD200 credit when you sign up.

What is botchat?

Not quite sure if this is the same as a chatbot, but this may help
https://en.wikipedia.org/wiki/Chatbot

PM-Track2-1_SMU - Deployment of Privileged Access Management for System Administrators

1. For the regular task that you are preforming as an admin, can you predefined without PAM?

As the accounts held by PAM are full administrative accounts, they will have full permission on those systems being accessed.

it might be better to restrict the accounts rights to the minimal permissions required to carry out the task instead of full admin rights.

2. Why CA is chosen? How about CyberArk comparison?

CA is mainly selected by management decision mainly due to price constraint in which we are not able to disclose at the moment. CyberArk is by far the market leader, but mainly it still depend on whether the particular product suit your organization need and requirement.

3. how do you protect and harden the PAM

Vulnerability scanning was performed and results where submitted to CA to verify issues. Patches that addressed the issues were applied.

4. Who is the vendor for the implementation?

Tindo Pte ltd

5. Is the PAM system with UI interface available

Yes, it has a UI available.

6. Do you define office hour that no approval is required for some administrator.

No , it is not restricted by the timing of access but defined by whether the system contains restricted data that requires approval to access.

7. What is the product name?

CA PAM

8. What's the duration (time-out) between the request and approval?

This is a customised setting. In our case the request for approval can be raised 3 days in advance

9. What product is SMU using?

CA PAM

10. won't this system cause bottle neck? how do you prevent or resolve this issue?

The remote sessions provided PAM is close to the native performance of RDP and terminal. Also the appliances are load balanced to reduce congestions.

11. What is the file size of the video recording session?

Due to video compression,it depends on the amount of changes made in the display. The rough sizing is about 0.5mb/min in our case.

12. can PAM bypass all required approvals in the event of emergency like DR?
In DR scenario, a PAM appliance is located in the DR site to provide access. In cases of total failure of the PAM, the master administrator account saved in a physical password envelope will be used to recover access for others.

13. What if the approver is away for meeting and the requestor (e.g. sys admin) needs to access the devices urgently?
There can be multiple approvers to grant access.

14. Is operation efficiency reduced? If yes to what extend?
Yes, there are some trade off between efficiency and security. In the new process. Admins will need to perform login to the PAM appliance along with 2FA to gain access to systems, for critical systems additional management approval are required.

PM-Track2-2_NUS nBox IHL CIO forum 2018 v2

1. Will the files on all devices be synchronised automatically for mobile, windows and MacOS?
   Yes, data is saved at the backend storage and synchronized across all endpoint and mobile platforms.
2. Do you block the USB port for staff end point with this nbox implementation?
   No, USB ports are not blocked at the moment. However, any USB storage devices plugged into an end point will get encrypted.
3. Can share the product or solution
   nBox is branded on Hitachi Vantara's HCP Anywhere product.
4. Can multiple users update edit a same documents at e same time? Like google doc?
   Multiple users can edit a doc at the same time. Assume 2 persons edits doc at same time and save it. 2 different versions would be saved. It is a different way of collaboration compared to other similar solutions such as Google docs where updates by multiple parties are shown in real time.
5. Why not use sharepoint for team sharing?
   Sharepoint have the same file sharing and collaboration capabilities as nBox. However, nBox allows data to be assessed anywhere and anytime (on both end points and mobile devices). In our organization, Sharepoint can only be assessed on the end points. If there is a need to review and approve changes to docs via a workflow, then Sharepoint would be employed for this use case.
6. Team folder storage is within the 1TB or a separate storage space.
   Separate storage space for team folders.
7. What did NUS use before the nbox solution?
   Depts could use either USB drives or other cloud solutions (not endorse by NUS IT).
8. how can the storage be grow? any upper limit?
   The storage backend is Hitachi's HCP, which is easily scalable.
9. Before nBox being selected,what are the other products being evaluated? Why nBox was selected?
   There wasn't a centralized file and sync solution before nBox and depts have their own internal solution to store and share data (ie, could be via USB drives or cloud solutions).
10. Did NUS compare with Microsoft Teams?
    NUS has OneDrive too but OneDrive is a cloud based solution. The concern with a cloud based solution is that data stored there would be replicated to many remote depositories. Even if the primary set of data is erased, we can never be certain that these replicated copies of data would be removed. Thus, data security is a concern.
11. Do NUS block USB port for your staff end user machine with implementation of nbox?

No, USB ports are not blocked at the moment. However, any USB storage devices plugged into an end point will get encrypted.

12. How do you generate a report to account for the various "share" over the months ?
    nBox's admin console is able to have an overall view of all the team folders created. Individual user's shared folders are managed by the user themselves.

13. What's disk space given to staff. Is the staff data backup by the enterprise system.
    Each staff is entitled to 1 TB of storage space.
14. What is the cost per user by providing 1TB per user?
    License is by number of users. In NUS case of 14k users, cost per user comes up to about $67 per user.
15. Any performance and stability issue ?
    None at the moment.
16. If the file being shared wrongly, can it be withdraw or disable the sharing immediately?
    The shared/team folders can be updated immediately to remove the staff who are not supposed to have access to the data.
17. What is the product used?

nBox is branded on Hitachi Vantara's HCP Anywhere product.

18. How do u backup the data?
    nBox has versioning capabilities. Each time a file is saved, a new file version is created (can have up to 10 versions). The file can be rolled back to any earlier version. We are also building a DR setup for disaster recovery purposes.
19. Is nbox a NUS developed solution or a vendor product?

nBox is branded on Hitachi Vantara's HCP Anywhere product.

20. Can you pls share with us the cost of implementing this solution

License is by number of users. In NUS case of 14k users, cost per user comes up to about $67 per user.

21. Is the nBox hosted on premise ?
    Yes, the entire nBox infra is setup on premise. Data saved in nBox stays in the NUS environment.
22. What was the implementation timeframe, 6 months or a year
    4 months from RFQ award to launch.
23. any restriction of file Types that can be stored?
    Admin defined restrictions. In NUS case, we do not allow pst/ost files to be stored in nBox due to the concern with large data sync to backend storage.
24. how NBox encrypt the data at rest?
    Hardware encryption.
25. How will the owners be informed if others make changes to the folder
    All the file updates are logged in nBox.
26. Is nBox off the shelf product ? If not, can share the product name?

nBox is branded on Hitachi Vantara's HCP Anywhere product.

27. What is the capacity given to each user? And total storage capacity in the server?
    Each user is entitiled to 1TB of storage. The storage capacity is 1.6 PB.
28. What is the product used for nbox?
    nBox is branded on Hitachi Vantara's HCP Anywhere product.

29. According to IM, files should not be shared among emd users, how did you manage to comply with IM?

There is no file sharing restrictions within NUS.

30. If you have internet separation, how do you transfer your files between Internet and Intranet environments?
    There is no internet separation in NUS.
31. how do you prevent data leakage using nBox?
    nBox is not DLP solution. There are separate DLP solutions that could help to address and prevent data leakage within the organization.
32. How big? What yt budget? Any backup?

Each user is entitiled to 1TB of storage. The storage capacity is 1.6 PB. License is by number of users. In NUS case of 14k users, cost per user comes up to about $67 per user.

nBox has versioning capabilities. Each time a file is saved, a new file version is created (can have up to 10 versions). The file can be rolled back to any earlier version. We are also building a DR setup for disaster recovery purposes.

33. how does nBox compare to existing solution such as onedrive, gdrive or dropbox? What prompted NUS to develop in-house solution that already exists in market?
    OneDrive, GoogleDrive and Dropbox are cloud based solution. The concern with a cloud based solution is that data stored there would be replicated to many remote depositories. Even if the primary set of data is erased, we can never be certain that these replicated copies of data would be removed. Thus, data security is a concern when data is hosted on the cloud. nBox is a on premise solution and data stored in nBox stays within the NUS environment.

PM-Track2-3_SIT Journey to the Cloud (with animation)

1. Would you recommend cloud provisioning and administration to be centrally managed or decentralize to various applications teams to self provision manage their own vpc for agility and accountablity?
   - this depends on your IT Governance requirements.
   - operationally & financially, would prefer to centralise the cloud account in order to benefit on usage discounts, etc. Then you can work on delegated access for scalability and centralised deployment of policy enforcements (i.e. AD GPO, end point protections, software & patch Management, etc).
2. How do you manage billing, subscription, budget, finance team?
   - Come up with the estimated cost of the resources you intend to use for your EPV (estimated procurement value)
   - Thereafter, perform regular usage review to anticipate possible topup or early renewal of the contract.
3. What are the challenges in meeting IM8 audit?
   - SIT is not bound to comply with IM8
4. Do u have an estimated cost saving using cloud after implementation. Any concerns migrate your corporate data in public cloud "in term IM8'"
   - SIT is not bound to comply with IM8
   - Estimated cost varies depending on the overall adoption and resources subscribed.
   - Savings is significantly seen when performing comprehensive cost comparison which includes the capital and operational cost of the on-premise data centre, hardware & resource availability & scalability, connectivity, reliability, manpower cost to maintain and refresh server hardware, etc.
5. Data encryption from app or db level? Will it affect performance?
   - Encryption can be done at both levels. It depends on the compliance and comfort level of the system owner and data classification requirements.
   - You need to strike a balance between security and performance.
   - You have the option to vertically scale up the size/specs of the instance (virtual machine) to improve performance.
   - Alternatively, if your application supports multiple servers, you have the option to horizontally scale the servers to improve both performance and availability.
6. What is the yearly subscription cost?
   - Subscription is quite subjective based on the resources subscribed and its usage.
   - Price list and price calculator are publicly available online in the respective CSP (cloud service provider) website.
   - Cost savings is definitely obvious as you basically pay for the service you actually use.
     - you can start with a lower server/storage spec and scale up as demand increases
     - alternatively, you can provision big for "critical systems" and slowly scale-down as you figure out the right specs of your servers/services with regular reviews or usage trend analysis.
7. What are the security measures for database servers to reside on cloud
   - Data at rest encryption (i.e. app / db / disk level)
   - Data in transit encryption
   - Secure Data in use method
   - Secure Remote Administration and auditing (i.e. site-to-site VPN, Direct Connect, Bastion Host, MFA, SIEM, PAM)

   - Secure Virtual Private Cloud setup (i.e. NACL, Routing, Firewall, NAT, etc)
   - End Point Protection
8. How do you measure cloud performance and troubleshoot issues?
   - There are a number of application load tester to measure cloud performance
   - When troubleshooting network performance, it's best to have someone who knows the entire cloud and on-premise infrastructure architecture in order to effectively identify the network segment in question.
   - AWS also has a built-in tool/service to monitor cloud resources usage and performance
9. Do you containarized the applications on the cloud?
   - SIT is considering the use of containers and we're already using serverless services for some applications.
10. Any fallback plan as if move back to on premise if need to?
   - SIT carry out regular backup of systems and data to an external backup storage (i.e. another cloud provider storage or on-premise) and have tested restoring such backup to another environment (i.e. on-premise vmware and another cloud provider) for such an extreme DR scenario as well as an exit plan from the incumbent CSP.
11. Can the data reside out of Singapore? If we use global HA
   - Some CSP allows you to keep your data within Singapore and some preassigned the DR region outside of Singapore.
   - If you're referring to Global HA, then it's expected that your data can reside out of Singapore.

PM-Track2-4_Analytics@TP

No questions were submitted.