Emory IT Architecture FY 2018 Priorities Presentation

Video

https://s3.amazonaws.com/emory-it-arch-demos/ItArchitecture.Overview2018.mp4

Transcript

<first slide>

Hello, this is Steve Wheat and I am Chief IT Architect for Emory University and Emory Healthcare. Welcome to this presentation on Emory's IT Architecture priorities for fiscal year 2018, which is September 2017 through August 2018. In this presentation, I will cover major initiatives for this fiscal year and the on-going functions of IT architecture that we will carry into the new fiscal year.

In the first slide, you'll notice the twilight of totality featuring the Great American Eclipse of 2017, which kicked off this year's planning cycle. Then we have our major initiatives, which are:

- Amazon Web Services;
- the IT Architecture Rotation Program;
- Mobile Apps;
- SOA, EDA, and FHIR Governance---that's a lot of letters, that is service-oriented architecture, event-driven architecture, Fast Healthcare Interoperability Resources;
- and a special focus on FHIR.
- And the last item is a summary of our on-going IT Architecture services and functions.

Let's drill down on the first item---AWS.

<next slide>

AWS is listed first, because it is arguably the largest piece of work on our plate for this year, and it has the greatest potential for IT Architecture transformation at Emory. There are presently two enterprise-wide AWS initiatives underway at Emory:

- the AWS Service for Emory Researchers Project
- and the On-premises to Cloud Migration Planning Project.

The AWS Service for Emory Researchers Implementation Project will execute on the feasibility studies, prototyping, and focus groups held in 2016 and 2017 to design a useful, secure, and HIPAA-compliant research platform on AWS for Emory researchers. In 2017 and 2018 Emory will implement and launch this service, offering AWS accounts and Virtual Private Clouds to research groups for delegated administration with central oversight and critical compliance and security controls.

The General On-prem to Cloud Migration Planning project will involve collaboration with other LITS units on design and feasibility of large-scale datacenter migration to AWS. Much of this in the coming year work will be design, feasibility, and proof-of-concept work much like we did for the AWS Research Service offering last year.

The main areas of focus for IT Architecture on the AWS Research Service Implementation Project are:

- The AWS Account ESB Service
- Emory/AWS DirectConnect Provisioning
- CIDR ESB Service
- Emory Elastic IP Service
- Virtual Private Cloud Provisioning (or VPCP) Web App

<next slide>

The AWS Account Service is an ESB service that does several things.

<next slide>

It exposes AWS API service operations to Emory orchestrations and applications and publishes events, which we can use to trigger other orchestrations and workflows at Emory. For example, this service is what we invoke to create type 1 and type 2 VPCs in an AWS account with CloudFormation templates, create an SAML Provider with the proper configuration so our Emory users can log into the AWS console with Emory Login, or an Account Alias so users can see a logical name for their account when they login instead of just the account number.

<next slide>

The AWS Account service persists account and VPC metadata and publishes events when this metadata changes. Emory has to keep track of who owns Emory AWS accounts, who the administrators are, what the purpose of the account is, what financial account number or speedtype the account is charged to, and more. This service stores that information and exposes an API to retrieve and manage that information for applications like the VPC provisioning web app and any other application that needs to know about or present this data.

<next slide>

The AWS Account service also persists AWS account billing data and publishes billing data events. Once AWS accounts are linked to a master payer account, line item billing detail is no longer available at the linked account level. So, in order to provide Emory AWS account owners with detailed billing information, we acquire the monthly bills for master payer accounts from these master payer accounts in comma-separated-value format and build AWS bill objects that are created in the AWS Account Service. This process accomplishes two major goals:

- First, AWS bill data is stored permanently in the AWS account service and can then be displayed at the linked account or master payer account level for individual account holders, administrators, or business managers at the departmental- or enterprise-levels
- Second, AWS bill events are published that can be used to trigger downstream integrations like building a flat file reflecting each bill's charges that can be loaded into the Emory financial system to attribute charges for each account to the proper financial account or speedtype specified by each account owner.

<next slide>

The next subproject of the AWS initiative is the AT&T NetBond ESB Service. This service enables the automation of the Emory to AWS DirectConnect provisioning. AT&T NetBond is presently Emory's provider of a direct network connection to AWS. DirectConnect provides a dedicated connection from an AWS customer to a specific AWS region. This type of direct connection provides a more consistent network connection to AWS and can increase bandwidth as opposed to connecting to AWS over the Internet.

<next slide>

The AT&T NetBond Service exposes the AT&T NetBond APIs and publishes events when API operations are performed, so that other Emory workflows and orchestrations can be triggered. In the future, Emory may use other or additional DirectConnect providers or products besides AT&T or this specific NetBond product. In that case, Emory will implement a similar service for each endpoint to expose the new provider or product APIs for DirectConnect provisioning automation.

<next slide>

The next subproject of the AWS initiative is the Classless Inter-Domain Routing or CIDR ESB Service. This service issues CIDR ranges to Emory AWS VPCs. CIDRs for Emory VPCs must be carefully managed to avoid conflicts on Emorys network and wasting Emory's private IP address space.

<next slide>

Emory's networking team registers CIDRs that are available for AWS VPCs in this service---either programmatically or using the VPC Provisioning Web App---and then this service can be invoked by the AWS Account Services provisioning orchestration to issue CIDRs to new VPCs as they are created.

<next slide>

The Emory Elastic IP Service is the next subproject of the AWS initiative. This service is necessary because Emory AWS users cannot make use of AWS public IP addresses or AWS Elastic IP address to make resources in their VPCs publicly accessible. This restriction is necessary, because Emory must route traffic through its own network or otherwise control ingress and egress to AWS VPCs to comply with Emory information security and regulatory compliance policies.

<next slide>

This service will be used to register public IPs that can be registered to Emory AWS VPCs. These IPs can then be mapped by Emory AWS users to private IP addresses they would like to expose to the Internet. This mapping request will result in a service request to Emory's network group to implement a static NAT for these two addresses.

<next slide>

The final subproject for IT Architecture is the Virtual Private Cloud Provisioning (or VPCP) Web Application. This application implements the user interface to Emory AWS account management, provisioning, and billing for Emory AWS users like researchers and systems admins in research groups and for central IT and information security administrators. The VPCP web app has 10 major functions, they are:

<next slide>

1. Manage AWS account metadata that is not available in the AWS console <next slide>
2. Manage CIDRs <next slide>
3. Manage CIDR assignments of CIDRs to VPCs <next slide>
4. Manage Virtual Private Cloud metadata that is not available in the AWS console <next slide>
5. Generate a new VPC (and allocate or generate a new AWS account, if needed) <next slide>
6. View current Emory firewall rules for VPCs <next slide>
7. Request new Emory firewall rules or changes to existing Emory firewall rules for VPCs. <next slide>
8. View existing Emory Elastic IPs for VPCs.<next slide>
9. Request new Emory Elastic IPs of changes to existing Elastic IP assignments. <next slide>
10. View detailed billing information for AWS linked accounts

So, the VPCP web app has quite a bit going on and will play a key role in implementing and managing the Emory-specific aspects of the AWS service for Emory researchers.

<next slide>

Moving on from the AWS project, our next major IT Architecture initiative for this year is the IT Architecture Rotation Program to bring technical staff from other groups into the IT Architecture team for three months at a time to work in depth on new or emerging technologies. The program will focus on the following areas this year:

<next slide>

AWS Account Provisioning

<next slide>

Emory's AWS VPCs and their structure, administration, and evolution

<next slide>

AWS serverless architectures, which allow us to develop applications that have no servers or middleware to manage or scale.

<next slide>

AWS MobileHub, which helps one develop and operate serverless backends for mobile and web apps and generates solutions to user and device identity management and authentication, which are otherwise costly and challenging to implement and manage over time.

<next slide>

Service-oriented, event-driven, and Fast Healthcare Interoperability Resources with current on-premises methods and new AWS architectures

<next slide back to main>

Our next major initiative is mobile apps…

<next slide to mobile apps>

Over the past three years Emory has gone from having and handful of mobile apps to sixty mobile apps we track in the portfolio. Emory maintains a dashboard of mobile apps and their status in the review and distribution process. To view the dashboard go to arch.it.emory.edu and check the quick links section at the top of the page. One of them is for Emory's mobile app dashboard. This page also has links to Emory's mobile app review and distribution processes.

The mobile app initiative this year focuses on four areas:

- The first area is the mobile app review and distribution process survey and improvement recommendations---Emory implementing policies and practices for internal and public mobile app distribution in 2014 and we've implemented tools and processes in 2015-2017 to make this all work and produce documentation of the mobile apps, their reviews and approvals, and distributions status. Now it is time to survey the institutional stakeholders and the app owners to help refine and improve the processes. <next slide>
- The second area is the preferred mobile app vendor program. The goal of this program is to improve the quality and security of mobile apps developed and Emory and ensure that they all can be maintained and have operational support. Over the past year, we structured program to identify preferred mobile app vendors, bring them up-to-speed with Emory's security and compliance requirements, and have them commit to specific mobile app architectures and processes articulated in a preferred vendor master professional services agreement. This year we need to conclude the process of on-boarding these vendors and communicate about the preferred vendor program broadly within Emory to drive new projects to these preferred vendors. <next slide>
- Third, we are working on reference implementations and documentation for using AWS MobileHub to develop mobile apps. This is a key part of our preferred vendor program to ensure that critical features like user registration, authentication, authorization, and auditing are done consistently and appropriately in Emory's mobile apps.
- Finally, we'll be developing reference implementations and documentation for AWS service-oriented and event-driven architectures for mobile and web app backends. This is another critical resource for the preferred vendor program and also provides valuable input for Emory's future integration strategies.

<next slide: back to main menu>

Our fourth main initiative is SOA, EDA, and FHIR Governance…

<next slide: SOA, EDA, and FHIR governance>

SOA and EDA governance is a framework for requesting and reviewing access to services and event to implement new integrations and recording and auditing these integrations that are implemented.

Again, these acronyms stand for: service-oriented architecture, event-driven architecture, and Fast Healthcare Interoperability Resources. FHIR, pronounced "fire," is really just a specification for specific use cases of service-oriented architecture for healthcare. We've listed it here at the top-level with SOA and EDA, because it is "hot" right now, pardon the pun. Emory is implementing a product from Cerner, our electronic medical record system vendor, called Ignite, which implements FHIR services to expose medical record information to third-party applications---either other vended apps or apps we build ourselves here at Emory. The prevalence of the FHIR specification in healthcare and our implementation of it this year is a major impetus for Emory to focus of SOA and EDA governance processes. We need to establish clear processes for requesting access to invoke Emory services, grant or deny that access, record those decisions, and audit our environments to ensure we're implementing those decisions.

Another major impetus for Emory to focus of SOA and EDA governance is the increasing need to automate cloud infrastructure and deployments for cloud implementations. Implementing cloud applications provided in the software-as-a-service or SaaS model and cloud infrastructure and platforms like AWS required integrating them with Emory identity, authentication, authorization, and other business data. Emory's ability to implement these integrations could be optimized with clear practices for requesting access to existing Emory ESB services, web services, and events.

Possibly the best motivation for looking closely at SOA and EDA governance is that while SOA and EDA is just emerging on the Healthcare side with the FHIR standard, Emory has been quite successful in developing consistent services and events on the University side for the past 10 years. Emory publishes over 50 ESB and web services with hundreds of service operations and events. Emory consumes many web services from external entities, although those are not as well inventories and documented as the services that Emory publishes. As part of the SOA and EDA governance initiative we are listing all of these in a format that can be readily understood by data stewards we identify for each service and event.

<next slide>

Typical stakeholders in a SOA and EDA governance process are:

- Data stewards
- Information Security
- Compliance
- Legal Counsel
- IT Operations

<next slide>

Requests to deploy and consume ESB services, web services, and events should be reviewed consistently and processed in a reasonable amount of time.

<next slide>

Emory should produce records and documentation of approvals and denials to deploy and consume services and events to verify and audit the use of ESB services, web services, and events.

<next slide>

There are some distinct considerations for internal-facing services…

<next slide>

…external-facing services…

<next slide>

…and vendor- or partner-provided services that Emory consumes.

<next slide: back to main>

The next major initiative for IT Architecture in the coming year is FHIR.

<next slide>

The Fast Healthcare Interoperability Resources specification from HL7 is a web services interoperability standard that builds upon the long-standing HL7 event-based interoperability standard. FHIR allows any vendor or organization to build web, mobile, voice, and other apps to a common request/reply web service specification and data resource model and have those apps work with multiple medical record systems that implement the FHIR specification. This creates new ecosystems and business opportunities around medical record and health information systems. For example, many vendors can now join Cerner's developer program and build apps that integration with Cerner's medical record and health information systems. For Cerner clients like Emory it means we have more choices and more capabilities. We will have more applications to choose from to address needs that Cerner might not otherwise prioritize. For our internal development projects, it means we have a robust, standard way to interact with Cerner's systems and present medical record data in our apps or update medical record data from our apps.

<next slide>

The first aspect of this initiative is to participate with EHC IT in the implementation of Cerner's Ignite solution, which is Cerner's implementation of FHIR for Millenium, Emory's medical record system.

<next slide>

The next part of this initiative is to create and document a FHIR reference mobile app to help guide Emory's developers and consultants in building mobile apps that talk to Emory's medical record system.

<next slide>

The final part of this initiative is to create and document a FHIR reference web app to help Emory developers and consultants build web apps that integrate with Emory's medical record system.

<next slide: main menu>

Our final slides outline IT Architecture's standing functions and services, which also consume a lot of our effort and focus each year.

<next slide>

There are six major functions and services, and contrary to our main graphic here we do not offer dog boarding, luggage check, or ferry boat rides…not sure how we came up with those. Our services and functions are:

<next slide>

- Cloud architecture and implementation consulting---working with projects and units looking to make the move into the cloud and AWS in particular. <next slide>
- Public mobile app distribution---IT architecture submits Emory mobile apps using Emory's official Apple, Google, and Amazon marketplace accounts and works with the marketplace contacts and the mobile app developers to complete vendor review and publish mobile apps. <next slide>
- Assist the UIT web team with internal mobile app distribution---while the web team does over 90% of the internal app distribution work using the Apperian platform as the Emory Mobile App Catalog, there are some certificate, credential, and key management work that IT architecture manages for internal app signing. <next slide>
- Mobile App Development---IT Architecture has developed four mobile apps over the past three years for Emory Healthcare and Emory research projects. As described in the previous section of the preferred mobile app vendor program, we are attempting to augment and redirect this capability with the preferred mobile app development vendor program. <next slide>
- Mobile App Governance---IT Architecture is a key player in the mobile app review and distribution policies, practices, and meetings to move mobile apps through the internal review process.
- Software development, support, and consultation---IT architecture has developed hundreds of foundation components, libraries, four mobile apps, thirty ESB and web services, and eight web apps over the past 10 years. We provide code support, training, and generally consulting for these products and developers and consultants working on these types of projects.

<next slide: main menu>

So, in review, these six initiatives comprise the bulk of our IT Architecture work for 2017 and 2018. We're particularly looking forward to launching the AWS service for Emory researchers and working closely with other Emory units in IT Architecture rotation. Thank you for your time and attention while watching this presentation. If you have any questions, please send them directly to me, Steve Wheat, at swheat@emory.edu or post your questions on the IT Architecture wiki at arch.it.emory.edu. Thank you very much!