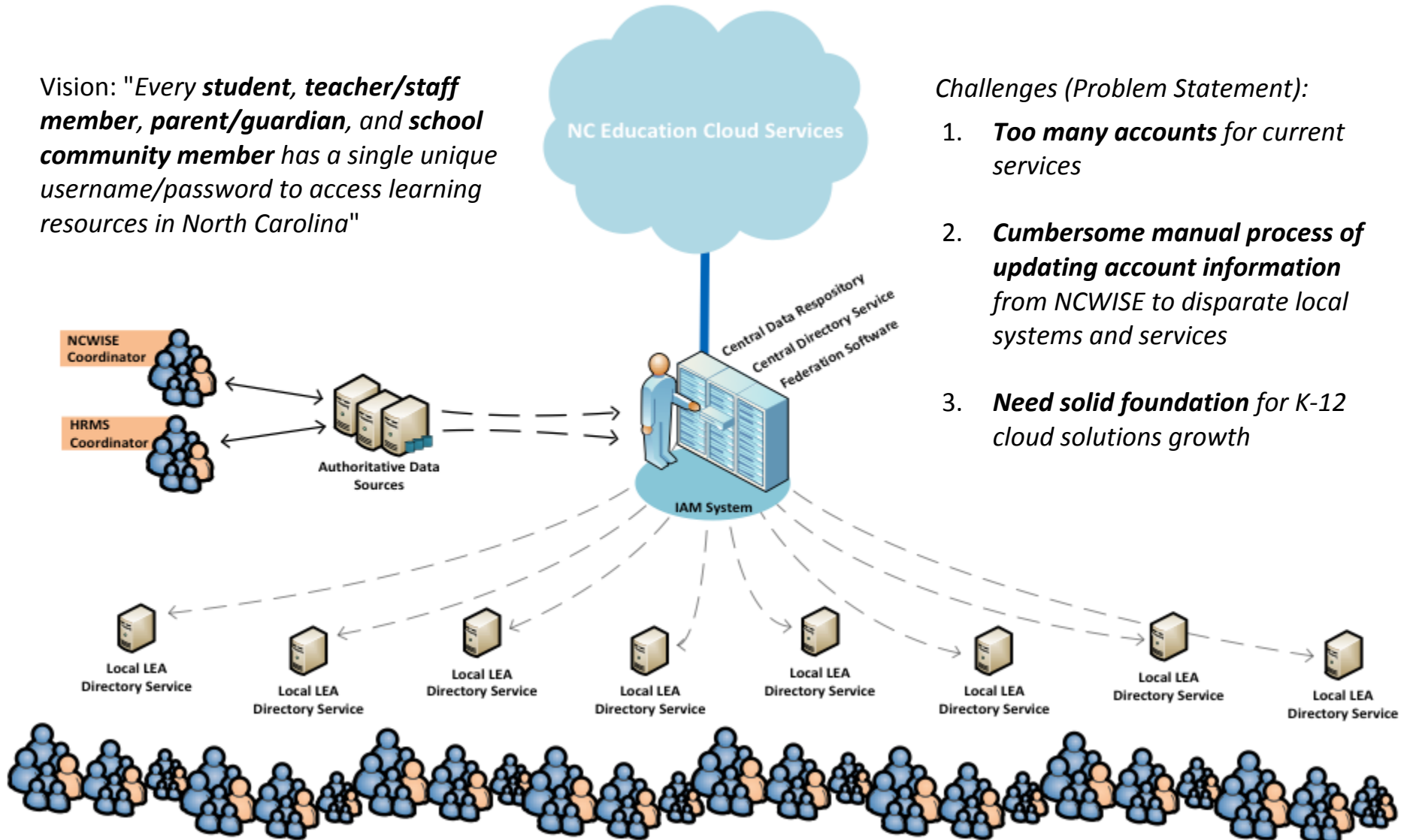# NCEdCloud IAM

Overview Presentation - July 2013

Recap: Recall the "Big Picture"

Vision: "*Every **student, teacher/staff member, parent/guardian**, and **school community member** has a single unique username/password to access learning resources in North Carolina*"

Challenges (Problem Statement):

1. ***Too many accounts*** *for current services*

2. ***Cumbersome manual process of updating account information*** *from NCWISE to disparate local systems and services*

3. ***Need solid foundation*** *for K-12 cloud solutions growth*

NC Education Cloud Services

NCWISE Coordinator

HRMS Coordinator

Authoritative Data Sources

Central Data Respository
Central Directory Service
Federation Software

IAM System

Local LEA Directory Service

Current Status

- The unanimous choice of the RFP evaluation committee was:

  - Identity Automation
  - http://identityautomation.com/
  - Recommendation was approved by DPI and ITS

- Contract was signed March 27, 2013, start date of April 1, 2013
- IAM-MS work is now underway!!
- Assessment Phase (due/completed April 30, 2013)
- Design Phase (due/completed June 30, 2013)
- Build Phase is now underway (as of July 1, 2013)
- Test, Deployment, Full Production Phases will follow

High Level Schedule of Project Phases

Phase I – Research and Planning
October 2010 – October 2011 (12 Months)

Phase II – Establish Service Model (included RFP Process)
November 2011 – May 2013 (18 Months)*

Phase III – Build and Implementation
Tentative Schedule: April 2013 – March 2014 (12 Months)

Phase IV – Full Production and Operation
Tentative Schedule: April 2014 - Ongoing

Procurement process took much longer than expected and delayed project

NCEdCloud IAM

Phase III - Build and Implementation Details

4/1/2013 - 4/30/2013: ASSESS *(DONE)*

- Develop Detailed Assessment Document

5/1/2013 - 6/30/2013: DESIGN *(DONE)*

- Develop Detailed Technical Implementation Plan

7/1/2013 - 7/31/2013: BUILD *(IN PROCESS)*

- Build compute / networking DEV infrastructure
- Build internal databases, applications
- Obtain access to initial authoritative data sources
- Obtain access to sandbox test environments for initial target apps

8/1/2013 - 9/30/2013: TEST

- Build compute / networking TEST infrastructure
- Migrate DEV environment to TEST
- Perform initial data load
- Build use case data
- Perform use case testing
- Build load testing infrastructure
- Perform use case, UI, load, data validation, fault tolerance testing

10/1/2013 - 3/31/2014: DEPLOY

- Build compute / networking PROD infrastructure
- Migrate TEST environment to PROD
- Enable automated testing
- **Final system integration with initial 5 target apps**
- **Early adopter LEAs and Charters on-boarded to initial 5 target apps**

NCEdCloud IAM

Phase IV - Full Production and Operation

- April 2014 and beyond

- All LEAs and Charters can subscribe to all of the initial five target apps starting April 1, 2014

- Up to ten additional statewide applications will be added during each subsequent year

NCEdCloud IAM

Key Organizations

NCDPI - NCEdCloud Sponsor

Friday Institute - NCEdCloud IAM Service Director

MCNC - NCEdCloud IAM Service Manager

Identity Automation - NCEdCloud IAM Service Provider

NCEdCloud IAM

Core Team

Sammie Carter
Friday Institute
NCEdCloud IAM Service Director

Mark Scheible
MCNC
NCEdCloud IAM Service Manager

Steve Thorpe
MCNC
NCEdCloud IAM Systems Analyst

Steve Hatch
Identity Automation
IdAuto IAM Service Manager

Troy Moreland
Identity Automation
*Chief Technology Officer &
IdAuto IAM Service Architect*

James Litton
Identity Automation
Chief Executive Officer

NCEdCloud IAM

Key Terms

NCEdCloud is the initiative responsible for providing services that include Identity & Access Management and Data Management

IAM-MS <u>was</u> the term for describing the service providing Identity & Access Management; it is <u>now</u> rebranded as ***NCEdCloud IAM***

Goals

Provide LEA faculty, students, parents and guests with a **single login** to all NCEdCloud sponsored systems, as well other cloud services that are utilized by numerous LEAs.

Provide **self-service** capabilities to all end users and delegation capabilities to all LEA administrators.

Provide LEAs a **standardized method to access identity data from NCDPI**.

User Statistics

Faculty: ~200K

Students: ~1.5M

Guardians: ~1.5M

Guests: *Unknown*

NCEdCloud IAM Components

Infrastructure, systems, services and resources responsible for providing the NCEdCloud IAM Service:

- My NCEdCloud
- NCEdCloud SAML IdP
- NCEdCloud IAM Sync
- NCEdCloud IAM Support Portal

NCEdCloud IAM

My NCEdCloud

- The interface for end users and administrators that will provide self-service and delegated administration capabilities

- *This service runs on Identity Automation's Access Request Management System (ARMS) product*

NCEdCloud SAML IdP

- The service that will provide single sign-on (SSO) capabilities to cloud systems that support the Security Assertion Markup Language (SAML) protocol and implementation.

- *This service runs on Identity Automation's Federated Identity Management System (FIMS) product.*

NCEdCloud IAM Sync

- The service responsible for managing the lifecycle of account management across all systems. (e.g. create, update, delete accounts)

- *This service runs on Identity Automation's Data Synchronization System (DSS) product.*

NCEdCloud IAM Support Portal

- The interface for end users and administrators that will provide incident management, change management, service catalog request and reporting capabilities

NCEdCloud IAM

NCEdCloud Username

Based on numerous constraints, an NCEdCloud Username* will be a randomly generated value with 4 alpha characters followed by 4 digits. The same username convention will be used by all user types (e.g. staff, student, parent/guardian, guest)

Example username: bgdr4159

* Note: While logins will use the 4+4 username convention, email address aliases be created can retain a more "user-friendly" convention

NCEdCloud IAM

Central Directory

The Central Directory is a component of the core infrastructure that provides a directory service for NCEdCloud IAM. The Central Directory is the authoritative source for the NCEdCloud Username and password. It is also the source of all target system integration whether by SAML, LDAP or direct provisioning.

NCEdCloud IAM

Target System Integration

Integration with target systems comes in three flavors:

- SAML
- Synchronization
- LDAP

The capabilities of the target system dictates the type of integration used.

Initial Target Systems

By March 2014:

- Google Apps for Education
- Central Directory Local Replica (CDLR)
- Zscaler
- Follet Destiny
- Discovery Education

Starting April 2014:

- Up to 10 additional targets per year

CDLR

- The Central Directory Local Replica is an optional local AD instance (within a district/Charter) that will be sync'd from the Central Directory - one way

- Responsibility for setting up the Windows Server 2012 VM or server to house the AD will reside with the LEA/Charter

- LEAs can point their local apps at this instance, if they choose, to enable their users to authenticate using their NCEdCloud Username

- Other LDAP directories can query the CDLR for user data

NCEdCloud IAM vs. HomeBase

- HomeBase includes applications such as PowerSchool, TestNAV, Truenorthlogic, SchoolNet, OpenClass
- NCEdCloud IAM will provide authentication to <u>many</u> cloud-based services, including (eventually) but not limited to HomeBase applications
- NCEdCloud IAM is a separate service from HomeBase application suite
- HomeBase is being rolled out in July 2013, while the NCEdCloud IAM becomes a production service on March 31, 2014
- Due to the scheduling constraints, the expectation is that NCEdCloud IAM may be used by HomeBase starting sometime after March 31, 2014

Early Adopters

NCEdCloud IAM Early Adopters:

- Participants
  - Small, Medium, Large LEAs and Charter Schools
  - Implementing between 2-5 of the initial Target Applications
  - Active participation in the IAM Working Group (required)
- Benefits
  - Ability to influence definitions of standards, policies, processes
  - Solves an immediate challenge/pain point for the LEA
  - More "directed" support than for later adopters
  - Would obtain earlier access to the CDLR (local AD) instance
  - Get the "hard work" of implementation out of the way earlier
  - Subsequent implementations would be easier
- Risks
  - Process may not be as smooth as later integrations
  - Slower "on-boarding" time, but less pressure to implement
  - Implementation efforts may not align with school calendar breaks

NCEdCloud IAM

Open Q&A + Contact Info

- Web site—place for FAQ, Guidelines, Presentations, Organization, Team members, news, links to DPI & others:
  - Now: http://cloud.fi.ncsu.edu
  - Starting Fall 2013: http://www.ncedcloud.org/

- Sammie Carter, swcarter@ncsu.edu, 919-513-8513

- Mark Scheible, mscheible@mcnc.org, 919-248-1997

- Steve Thorpe, thorpe@mcnc.org, 919-248-1161