Access to CareData

Even though this document is almost entirely focused on the Snowflake security and access control, the access to remainder resources also suffer from the same challenges – lack of an industrial strength solution.

Snowflake security and access control are of paramount concerns. However, at OptumCare they are not being addressed adequately. It is not because of lack of knowledge, experience or being aware of vulnerabilities they pose and inefficient resource consumption they present. Instead, the decisions are made at some other part of the organization that we need to abide by.

There is a lack of an enterprise grade solution that provides federated authentication, single sign-on and MFA capabilities for internal and external users. In lieu of that, the DWaaS has been trying various solutions and presenting them to the EIS group and other stakeholders. Unfortunately, all those solutions keep getting rejected. To compound the problem, it is almost impossible to get all those stakeholders in a meeting, so that they can all come to a consensus. But that is proving to be a challenging task.

The latest patchwork of a solution is – 1. for integrated users, users need to create a Secure request to get access to the Snowflake. The accounts are created automatically when an access request is made in Secure; 2. Non-integrated users are invited by email. Non-integrated users are also using email id but, they must use their password along with the email id. They are setup as local users.

Note: *this is not a long-term solution due to its many deficiencies. It will be replaced as soon as an enterprise grade solution is available.*

The following are my notes from the meetings I’ve attended, and they have been validated by the participants. Even though they clearly show that there has not been much progress made on this subject, but it is not because of lack of trying, but there is no substitute to the enterprise grade solution.

+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++

Meeting with John Shin, DWaaS team and Anthony Andersland

Meeting on 12/17/2020 with John Shin, DWaaS team and Anthony Andersland

Subject: Snowflake Security and login

John Shin is the Snowflake main resource.

John Shin security, the rest of the DWaaS

Anthony Andersland Anthony Andersland

Atif is the second in command

Teresa Black's Snowflake acct.: <https://optum_poc.east-us-2.azure.snowflakecomputing.com/console/login#/?returnUrl=internal%2Fworksheet>

CDO's and areas:

Machine generated alternative text:
Search 
Neutral 
14 
16 
18 
20 
21 
22 
23 
24 
26 
27 
28 
29 
31 
recopy • 
Painte 
Form 
Group 
Califomia 
Califomia 
Colorado 
Florida 
New Mexico 
Washington 
Washington 
Col o rado 
Washington 
Help 
JIVE 
ACROBAT 
Table • 
ANN 
APPLECARE 
HO-CA 
8 Hcp-co 
HOP-FL 
HCP_NM 
HCP-wzvNPN 
HCP.WA.TEC 
MEDEXPREss 
MONARCH 
NEWWEST 
OMN-CA 
OMN-NJ 
o MN-UT 
OMN-AZ 
PR OH EALTHCT 
PROHEALTHNY 
RELIANT 
RIVERSIDE 
SMA 
usMD 
WELL MED 
CDO Summary 
Reg 
Southwest 
Southwest 
Southwest 
Mountain West 
Central 
Mountain West 
Pacific Northwest 
Pacific Northwest 
East 
Southwest 
Mountain West 
Southwe st 
Mountain West 
South "e st 
Mountain West 
Mountain West 
East 
Mountain West 
Pacific Northwest 
Central 
Feed to DL Feed 
(Y/ N) Frequency 
American Health Network (ANN) 
Applecare 
Legæ/ CMG - Magan 
Homecare Dimensions 
HQlthCare Par-tneÆ CA (6 
Hcp CO 
Hcp. NM 
HO WA- Phßcians Netwk (NPN) 
WA. The Everett clinic (TEC', 
Med 
Monarch HealthCare 
Mounta.n MediGl G 
NAMM California 
Ph"ici.ns 
(CO-MVMGJ 
OptumCare Medical Group Of California 
of CT 
OptumCare Network Of NJ 
of Utah 
OptumCare Network Of Arizona 
physicians (CT) 
Reliant Medical Group 
Surgical Care Associates (SCA) 
(SMA, NV) 
The POLYCLINIC (Tpq 
usMD 
wellMed (TX and FL) 

+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++

**Meeting 1/6/2021 with Atif on Login**

The purpose of this meeting is to understand the intricacies among Azure Active Directory, guest users, access policies, Snowflake and other resources

• How is AAD is configured, e.g., single sign-on?

• How are guest users setup, e.g., in groups or individuals?

• How are the access policies managed, at the group level policy or individual level policy?

• How is authentication and authorization implemented between AAD guest users and the Snowflake?

• Does a guest user has to login to each service individually or login once and then access all services that the user has access to, based on their permissions, of course, e.g., single sign-on? Can an authenticated user access any other resources, e.g., a blob store, a VM, etc.?

• Are guest users only authorized to access Snowflake or any other resources as well?

• If only Snowflake, then how is access to any other resources authorized?

• Is there only one way to authenticate a user and access Snowflake - thru AAD guest user or there are more ways to ways?

• If more ways, which ones?

+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++

**Meeting 1/7/2021 with Atif**

Subject: Non-integrated logins

spoke with Atif; we're both on the same page in terms of concerns; he has agreed to give me weekly status update

+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++

Note: Since 1/14/2021, reached out to Atif on regular basis about any updates. His response was almost always the same – No new updates.

+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++

**Meeting 3/29/2021 with Pierre, David Smith (David declined)**

**Subject: Snowflake login**

DWaaS team is responsible for the Snowflake login

Until recently, they were doing the local Snowflake accounts

An AAD is setup in the Azure platform

DWaaS are managing the AAD user accounts

For integrated users, users need to create a Secure request to get access to the Snowflake. The accounts are created automatically an access request is made in Secure

Non-integrated users are invited by email. Non-integrated users are also using email id but, they have to use password along with the email id. They are setup as local users. There are quite a few of them. *This is not a long-term viable solution and there no long-term plans just yet*. For example, Pierre requested a couple of service accounts in Secure a few days ago. He was told, they need to have email addresses and they are treated as non-integrated users

Chewbacca team David Smith and Pierre Fortin are managing user accounts in AAD

It is all in the POC environment

All these user accounts are created in the PoC environment, which is a pseudo production environment

DWaaS is creating accounts in POC. It is a streamlined but slow process

For non-integrated users, requests come from their manager

Question: How does to modifications for the non-integrated users work?

Response: Pierre gets email requesting modifications and he makes the requested changes

*Note: There is no review, approval and audit process as of yet*

Smokey team gets involved to address vulnerabilities

Yoda and Chewbacca teams are converting it from PoC (pseudo production) to Production

++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++

**Meeting 3/30/2021 with Atif Al-Amir**

**Subject: Snowflake login**

They have tried several different solutions based on current context and research

Three different teams are involved plus the general EIS. They have never been able to get them together in a meeting to come to some consensus

They're getting different messages and different directions from different groups

Dan P. got involved and escalated the issue. As a result, a meeting has been scheduled for this or next week.

They invited two group from the IIM team, they have all accepted the invite, now hope that they will show up to the meeting.

The following are the latest approaches to solve this problem:

1. When they tried external users, federated authentication kicked in and they could not login. These users were from DaVita Medical Group. John L. suggested to get in touch with EIS group. Rajesh is trying but, without much luck
2. One user from David Meditz team had Citrix, tried it and it worked as expected via Citrix. But, the EIS rejected that approach due to scalability concerns
3. They give resource addresses to try them, but without permissions
4. The VPN addresses provided did not work

Bottom line: Worst case scenario, if no solution works, then use local accounts. Not the long-term viable solution.

Note: *Atif won't be much longer at OptumCare. Main reasons: frustration and lack of available help*