ITS Strategic Roadmap – FY20 Planning

Identity & Access Management

Author: *James Zaletel*
Date last updated: *December 27, 2018*

Background

Identity and Access Management technology allows for users to securely log into the Metro network, access information and allow Metro to better and more efficiently secure the devices used by Metro departments. Metropolitan Government has standardized on a set of solutions to ensure security throughout Metro. The Microsoft tools used in this mature space include:

- Active Directory Domain Services (ADDS)
- Active Directory Federated Services (ADFS)
- Microsoft Azure Active Directory (Azure AD)
- Domain Name Services (DNS) for internal and external DNS management
- Group policies
- Active Directory Certificate Services (ADCS) used for the Metro Private Key Infrastructure (PKI)

Metro ITS is responsible for maintaining the overall health of the Active Directory infrastructure. However, there are currently multiple Microsoft Active Directory domains across Metropolitan Government departments and agencies:

1. Metro ITS provides Active Directory Domain Services, ADFS, DNS services, group policy management, and Active Directory Certificate Services for Metro general government department employees, primarily those that are under the executive branch, but also a number of elected officials including the Davidson County Clerk, Metro PD, Property Assessor, Trustee and Register of Deeds.
2. The Davidson County Sheriff's Office (DCSO) provides Active Directory Domain Services and group policy management and support for Sheriff's office staff. Metro ITS provides DNS support and Active Directory Certificate Services for DCSO.
3. The Justice Integration Services (JIS) department provides Active Directory Domain Services and support for staff of the various judicial agencies, including Criminal Court Clerk, General Sessions, Chancery Court, District Attorney, and others. Metro ITS provides DNS support and Active Directory Certificate Services for all of these agencies.
4. The Metro Nashville Public Schools (MNPS) fully supports their own Active Directory Domain Services, DNS, group policy and certificate services infrastructures.

These services are used by all of Metro and are foundational services, key to the business processes used by departments. With such a wide array of customers, the team's focus is on reliability, consistency and ever-increasing capability when it comes to the solutions and services provided.

Current Strategic Drivers

1. **Customer Demand: Cloud-based Services** (Game-changing) – Use of external cloud-based services requires robust identity systems. Continued emphasis on "identity" and the impact of dealing with external parties and cloud service providers, such as Microsoft, will drive the need to develop some level of federated services around identity.
2. **Customer Demand: Secure Government Systems** (High) – With massive data breaches in the news on a regular basis, we must strive at all times to protect the security, availability and integrity of all data entrusted to our management.
3. **Technology Change: Multifactor Authentication** (High) – Industry push to the use of advanced/multi-factor authentication methods. Identity industry projects an emphasis on providing alternative means to authenticate identity as well as the need for dual-factor authentication and/or location based authentication solutions to strengthen the security of this service.
4. **Technology Change: "Identity" as the New Firewall** (Game-changing) – The collective impact of multiple IT strategies (Cloud, mobility, smart and connected products) has limited the effectiveness of network based perimeter defense, making "identity," the ability to securely provision and de-provision access to information and services, authenticate users and devices, and conduct real-time monitoring and alerts related to malicious activity, an increasingly important method of securing information and services. Additionally, the targeting of internal privileged accounts, which have an increased value to malicious perpetrators, has been propagating.
5. **Customer Need: Streamlined Authentication Methods** (High) – Customers have asked for single sign on capability, which would reduce the need for Metro's staff to remember multiple passwords. The use of federated services to allow access to externally hosted applications continues to grow

On the Horizon Strategic Drivers

1. **Regulatory Compliance Obligations** (High) – Proposed changes to certain regulations and standards such as HIPAA/HITECH and PCI-DSS call for greater control of, and visibility into, the use of "privileged" accounts.
2. **Industry Trend: Online Access to Government Resources and Services** 🟦🟨🟩 (Game-changing) – As government becomes more digital, digital identity will need to become more reliable in order to serve as the core for all digital transactions. A public authentication account is needed to provide a secure domain to enable citizens to access these core resources or services.

Short Term Goals (0-6 months) 7/1/19 – 12/31/19

#	Goal/Objective	Est. Start	Est. Duration
1	Begin Phase one for the Provisioning Project (planning for user provisioning), which would allow identify authoritative sources for certain user data, populate the AD account with that data and allow for automated user account provisioning.	7/19	6 Months
2	Investigate Azure Information Protection to utilize Azure Rights Management in the protection of information across devices.	7/19	12 months
3	Continue work with other teams on a public authentication account initiative for access to Metro Government services.	7/19	6 Months
4	Expand Metro's Azure Active Directory capabilities, develop and deploy solution for systems in the Azure Government Cloud.	9/19	12 Months
5	Research and evaluate need for privileged account management (PAM) or privilege elevation and delegation management (PEDM) solutions. Provide report to ELT on findings. (capital funding required)	11/19	6 Months
6	Evaluate and research use of Microsoft Identity Manager (MIM) to implement B2B and B2C solutions for third parties. Provide report to ELT on findings.	10/19	6 Months

Medium Term Goals (6-18 months) 1/1/20 – 12/31/20

#	Goal/Objective	Est. Start	Est. Duration
1	Begin Phase two for Provisioning Project (implementation).	3/20	6 Months
2	Research and evaluate RBAC (Role Based Access Control) which would allow for ease of user provisioning and apply the principle of least privilege to all accounts. Provide report to ELT on findings.	6/20	6 Months

Long Term Goals (18-36 months) 1/1/21 – 6/30/22

#	Goal/Objective	Est. Start	Est. Duration
1	Evaluate and assess use of Risk Based Authentication mechanisms	1/21	6 Months
2	Research and evaluate standardized governance model adoption across all domains and report findings to ELT.	1/21	12 Months

Related Roadmaps

- Information Security Management
- System Lifecycle Management
- Field Services

Related Resources

- Connected Nashville
- Executive order 034
- Microsoft Cloud Platform Roadmap
- State and National Trends of Two-Factor Authentication
- Best HIPAA Compliance Password Policy
- PCI Security Standards
- Microsoft Identity Manager Roadmap
- Microsoft's Identity Life Cycle Management Strategy And Roadmap