Analyst III, Identity and Access Management Active Directory Administrator

Forbes includes U of G Among Canada’s Best Employers
Professional and Managerial Group

Analyst III, Identity and Access Management Active Directory Administrator

Computing and Communications Services (CCS)

Hiring #: 2022-0209

Please read the Application Instructions [1] before applying

Computing and Communications Services (CCS) is the central IT department at the University of Guelph, providing core IT services and technology solutions to the University community. CCS has a progressive organizational culture, including a strong learning and development focus, and is committed to its Core Values: Service Culture, Integrity, Individual Leadership, Teamwork, Agility, and Communication.

One of the important functions of CCS is providing Identity and Access Management (IAM) services for platforms and applications used by the entire University of Guelph community. Active Directory is a critical component of our infrastructure and provides authentication and authorization services to many of the critical applications used on campus, including the University website, email, learning management, and several enterprise applications.

The successful candidate will support and advance directory and access management services at the University of Guelph, with a particular focus on Active Directory and Azure Active Directory. Services provided by the Identity and Access Management team enable authentication for over 25,000 unique users daily, protect hundreds of on-premise websites, and facilitate federated single sign-on with almost 80 cloud and on-premise service providers and dozens of other service providers via the Canadian Access Federation. Responsibilities of this role include maintaining service levels, integrating new services, and evolving Active Directory and other components of our access management infrastructure. The role also includes providing technical support and guidance to a wide range of campus community representatives including CCS, faculty, staff, students, and distributed IT staff on campus.

The ideal candidate for this role will have five or more years of experience supporting and administering Active Directory in a large environment, with experience managing Azure Active Directory. Leveraging a solid technical background, experience in scripting and programming, and a customer focused mindset, they will be an integral member of the Identity and Access Management team that oversees all aspects of the identity lifecycle at the University and provides technical support for several key applications that provide authentication and authorization services for applications used across campus. The successful candidate will help support the tools that we have in-place today and work on projects within CCS to improve services for the future.

Responsibilities of this position include:

- Providing technical support for our Active Directory, Azure Active Directory, and web access management services with excellent customer service to our clients across campus
- Working collaboratively with CCS teams, other organizational units on campus, and 3rd party/cloud service providers to integrate their services into the University’s web access management platform.
- Investigating, troubleshooting, tracking, and resolving access management related issues
- Participating in a variety of projects related to our access management tools, technology, and processes
- Providing input on technical direction and new technology adoption within CCS and the Identity and Access Management team
- Following proper change management processes to keep servers and applications updated and secure
- Developing tools, writing scripts, and automating processes to assist with routine tasks, most commonly in PowerShell.
Requirements of the position include:

- Bachelor’s degree in Computer Science/Information technology and a minimum of five years of related work experience, or an equivalent combination of education and experience
- Systems administration experience on Windows Server operating systems
- Strong experience managing a large on-premise Active Directory implementation
- Experience with Azure Active Directory for Identity and Access Management in Office365, including Azure Active Directory Connect, ADFS, Azure MFA, and AD CS/PKI
- Experience provisioning identities and groups in Active Directory or Azure Active Directory using custom scripts, SCIM, or third-party identity governance tools
- Hands-on technical experience supporting web servers including configuration, troubleshooting, and ongoing performance monitoring
- PowerShell scripting experience
- Strong analytical, interpersonal, technical writing, and communication skills with ability to work effectively with non-technical business clients, technical team members, and third-party support
- Understanding of IT security best practices
- Ability to balance the competing demands of multiple projects and operational requirements
- Ability to work individually and as an integral member of a high-performance team

The following optional skills and experiences will set a candidate apart:

- Previous experience supporting other directory services, such as LDAP
- Hands-on technical experience with web access management and identity federation solutions, such as Shibboleth and Oracle Access Manager
- Hands-on technical experience supporting Java application servers, such as WebLogic, Tomcat, and Apache, including configuration, troubleshooting, and on-going performance monitoring
- Experience in web application design, ability to integrate with a wide range of web application platforms, and understanding of the HTTP protocol
- Application development experience in Java or a related platform
- Familiarity with protocols such as SAML and REST
- Administration of Oracle databases or other relational databases
- Previous work experience in a higher education institution
- Relevant technical certifications

Position Number         681-008  
Classification               P04*  
Professional/Managerial Salary Bands [2]  
*Tentative evaluation; subject to committee review.

At the University of Guelph, fostering a culture of inclusion [3] is an institutional imperative. The University invites and encourages applications from all qualified individuals, including from groups that are traditionally underrepresented in employment, who may contribute to further diversification of our Institution.

Posting Date: 2022 03 28  
Closing Date: 2022 04 25 (extended)

Source URL: https://www.uoguelph.ca/hr/careers-guelph/current-opportunities/analyst-iii-identity-and-access-management-active-directory

Links
[1] https://www.uoguelph.ca/hr/careers-guelph/how-apply  