



JOB DESCRIPTION

Post Details:

Post Title:	Principal Technician (End User Devices)	Organisational Element: NATO Digital Workplace Centre
		Job Family: Digital Backbone Engineering
Rank/Grade:	G12	
Military/Civilian:	Civilian	Location: Braine-l'Alleud, BE

Organisation context:

This is a position within the NATO Communications and Information Agency (NCI Agency), an organization of the North Atlantic Treaty Organization (NATO).

To strengthen the Alliance through connecting its forces, the NCI Agency delivers secure, coherent, cost effective and interoperable communications and information systems in support of consultation, command & control and enabling intelligence, surveillance and reconnaissance capabilities, for NATO, where and when required. It includes IT support to the Alliances' business processes (to include provision of IT shared services) to the NATO HQ, the Command Structure and NATO Agencies.

Organisational Element Statement of Functions:

NATO Digital Workplace Centre (NDWC) is accountable to the General Manager for the consolidated Agency consultation and collaboration services that comprise the current Digital Workplace, covering the operational NATO services, across all content classifications and security domains, for desktop computing, mail, instant messaging, video teleconference (VTC), content services platforms, telephony, printing and mobility services. Responsibilities also cover the organisation and support of all digital events, meetings and large-scale conferences for both the Agency and NATO stakeholders. Furthermore, the NDWC also has the responsibility for driving the future roadmaps of these services across the NATO Enterprise to enable a NATO Digital Workplace through new services.

The NDWC is led from its headquarter location in the Agency campus in The Hague (Netherlands). The majority of the technical staff and technical capabilities are located in Agency facilities in Mons, Brussels, Braine L'Alleud (Belgium) and Oeiras (Portugal).

The Personal Workspace (PWG) provides a persistent, shared conversational workspace that helps NATO staff initiate, organize and complete their daily work. The Personal Workspace Group is responsible for the lifecycle and in-service support of End-User devices (i.e. Desktops/Laptops/Tablets), Mail, Skype and Mobile Telephony services across the NATO Enterprise. In close coordination with local support teams, Personal Workspace team's focus is to provide 24/7 timely response to Incidents and Service requests coupled with a continuous effort to provide end-users with a state-of-art digital work experience.

Job role description:

The Digital Collaboration Technicians are responsible for managing and maintaining digital collaboration tools and platforms within an organization. They oversee the implementation and integration of these tools, as well as provide technical support and training to users. They specialize in deploying communication and collaboration software, such as video conferencing systems, team messaging applications, and document sharing platforms to create seamless virtual work environments. Their role involves configuring these tools to ensure coherent integration and user-friendly experiences, troubleshooting technical issues, providing user support, and staying up to date with the latest collaboration technologies, to enable teams to work cohesively, regardless of their physical locations, in order to foster a connected and productive digital work environment. This role requires a deep understanding of collaboration technologies and expertise in various digital collaboration platforms. It requires the ability to work closely with other IT professionals and business stakeholders, and strong communication skills to effectively collaborate with cross-functional teams.

Duties and Responsibilities:**Systems integration and build:**

- Provides technical expertise to enable the configuration of system components and equipment for systems testing;
- Collaborates with technical teams to develop and agree system integration plans and report on progress;
- Defines complex/new integration builds;
- Ensures that integration test environments are correctly configured;
- Designs, performs and reports results of tests of the integration build;
- Identifies and documents system integration components for recording in the configuration management system;
- Recommends and implements improvements to processes and tools.

Application support:

- Maintains application support processes, and checks that all requests for support are dealt with according to agreed procedures;
- Uses application management software and tools to investigate issues, collect performance statistics and create reports.

Systems installation and removal:

- Installs or removes hardware and/or software, using supplied installation instructions and tools, including handover to the client;
- Uses standard procedures and diagnostic tools to test installations, correct problems, and document results;
- Records details of all components that have been installed and removed;
- Assists users and follows agreed procedures for further help or escalation;
- Contributes to the development of installation procedures and standards.

Specific duties for this post:

- Support cloud-based endpoints and remote access technologies;
- Monitor system health, analyse alerts, and tune thresholds;
- Maintain device compliance and reliability;
- Provide expeditious Level 2 and Level 3 support services (including technical support to service desk and emergency on-site assistance) to ensure Personal Workplace services remain operational;
- Participation in Incident Management, Service Request management;
- Assist with deployment and optimisation of virtual desktops;
- Support endpoint security solutions including Trellix;
- Generate inventory and compliance reports;
- Monitor and respond to security events;
- Participation in incident, problem, and change management processes;
- Develop PowerShell scripts for automation and remediation;
- Provide inputs to Service Delivery and Service Improvement Plans as a SME;
- Stay abreast of technological developments relevant to the area of work such as Cloud technologies and Security;
- Deputize for higher grade staff if needed;
- Perform other duties as may be required.

Education, Experience and Training (essential):

Education:

Higher vocational training in a relevant discipline with 3 years post-related experience. Or a secondary educational qualification with 5 years post-related experience.

Experience:

- At least 3 years' experience implementing, managing, and optimizing collaboration tools and platforms within a digital ecosystem of an organization;
- Demonstrable knowledge of IT infrastructure and systems, including enterprise-class servers, operating systems, storage, and virtualization technologies;
- Practical experience of Endpoint & End User Support, Cloud & Virtual Desktop Support, Security & Endpoint Protection, Scripting & Automation and Monitoring & Observability;
- Experience with SCOM, Zabbix, Lansweeper, and SCCM;
- Good experience deploying communication and collaboration software;
- Very good experience with troubleshooting and providing end users' support;
- Very good problem solving and communication skills.

Education, Experience and Training (desirable):

Experience:

- Working knowledge in system management automation and monitoring;
- Experience with Modern Endpoint management solutions like Intune or similar;
- Cloud endpoint and VDI experience;
- Experience with SCOM, Zabbix, Lansweeper, and SCCM tools;
- Endpoint security experience (Trellix);
- Working knowledge in system management automation and monitoring;
- Knowledge of observability and asset lifecycle management best practices;

- Good understanding of Application security, Internet security and IT data protection mechanisms;
- Awareness of industry's latest technology trends and applications, such as Cloud Applications and Security;
- Relevant IT certificates (Microsoft, Security, Endpoint or Cloud focused);
- Good understanding of Application security, Internet security and IT data protection mechanisms;
- Awareness of industry's latest technology trends and applications, such as Cloud Applications and Security;
- Technical certification in Communication and Collaboration systems: MCSE or equivalent;
- ITIL v3/v4 Foundation certificate;
- Prior experience of working in an international environment comprising both military and civilian elements;
- Knowledge of NATO responsibilities and organization, including ACO and ACT.

Behavioural competencies:

- *Delivering Results and Meeting Customer Expectations* - Focuses on customer needs and satisfaction; sets high standards for quality and quantity; monitors and maintains quality and productivity; works in a systematic, methodical and orderly way; consistently achieves project goals.
- *Applying Expertise and Technology* - Applies specialist and detailed technical expertise; uses technology to achieve work objectives; develops job knowledge and expertise (theoretical and practical) through continual professional development; demonstrates an understanding of different organisational departments and functions.
- *Creating and Innovating* - Produces new ideas, approaches, or insights; creates innovative products or designs; produces a range of solutions to problems.

Language:

A thorough knowledge of one of the two NATO languages, both written and spoken, is essential and some knowledge of the other is desirable.
NOTE: Most of the work of the NCI Agency is conducted in the English language.

Travel:

Business travel to NATO and national (NATO and non-NATO) facilities as well as frequent travel between the NCI Agency offices.
 May be required to undertake duty travel to operational theatres inside and outside NATO boundaries.

Work Environment:

Normal office environment.