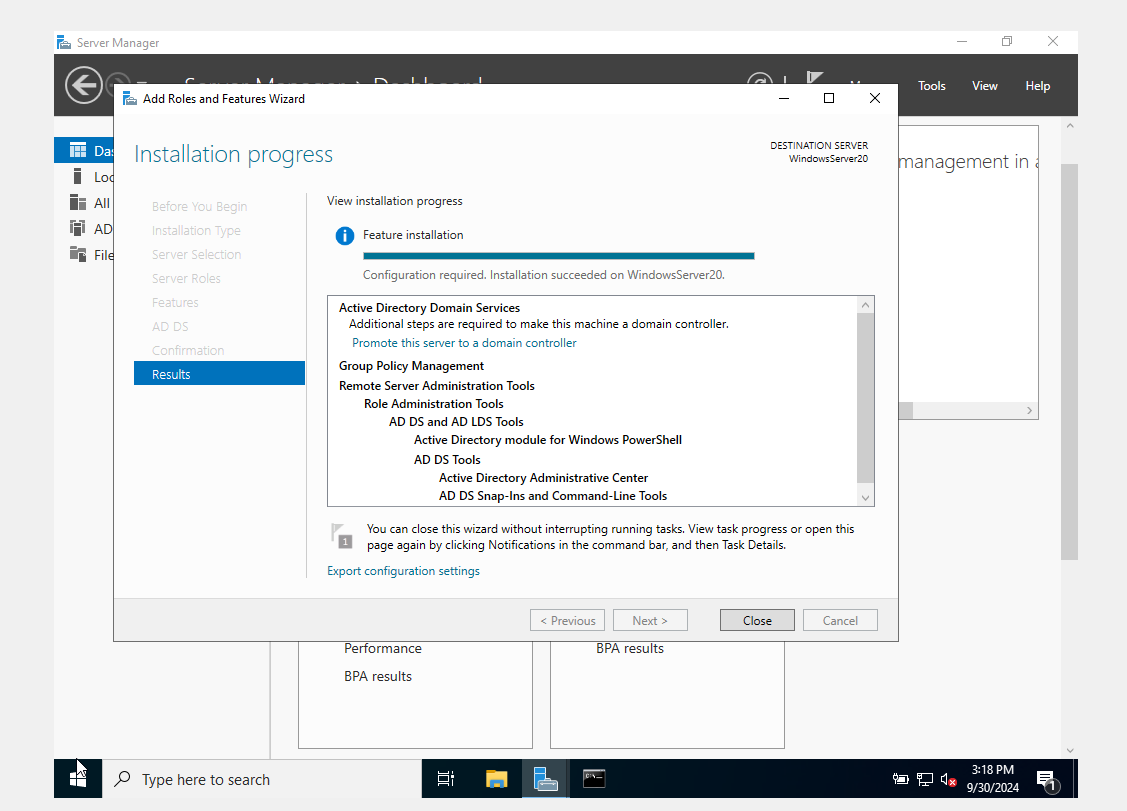
**Real Case Scenario**

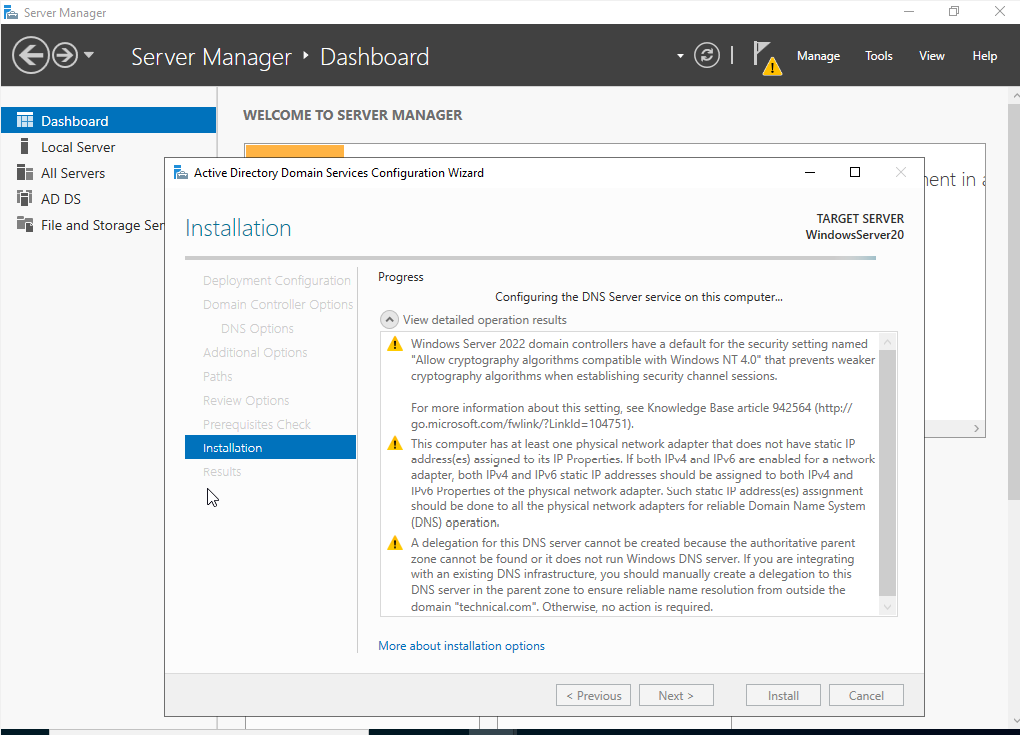
Taylor needs to create a domain controller in Active Directory. Follow the instructions below and ensure the proper information is added to the ticketing system. This is a medium-priority request assigned by the system administrator. The ticket will be under Ashley T. Since she doesn’t have a work email set up yet, she will use an established work email: ashwork@comcast.net.

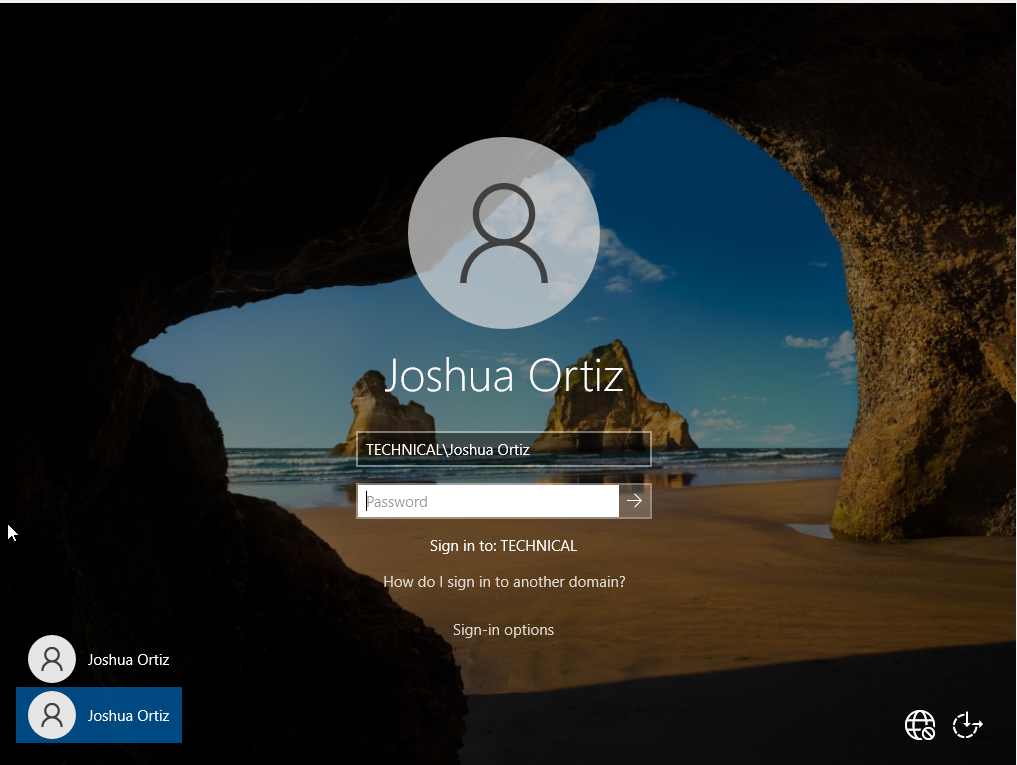
**Instructions to Create a Domain Controller:**

1. **Install Active Directory Domain Services (AD DS):**
   * Open Server Manager.
   * Click on “Add roles and features.”
   * Select “Role-based or feature-based installation” and click “Next.”
   * Choose the server you want to promote to a domain controller and click “Next.”
   * Select “Active Directory Domain Services” and click “Next.”
   * Complete the wizard and install the role.



1. **Promote the Server to a Domain Controller:**
   * After the installation, click on the notification flag in Server Manager and select “Promote this server to a domain controller.”
   * Choose “Add a new forest” and enter the root domain name (technical.net).
   * Set the forest and domain functional levels and provide a Directory Services Restore Mode (DSRM) password.
   * Complete the wizard and restart the server.





**Adding Information to the Ticketing System:**

1. **Create a New Ticket:**
   * Open the ticketing system and create a new ticket.
2. **Enter Ticket Details:**
   * **Title:** Create Domain Controller in Active Directory
   * **Description:**  Taylor needs to create a domain controller in Active Directory following the provided instructions. This is a medium-priority request assigned by the system administrator.
   * **Assigned To:** Ashley T.
   * **Email:** ashwork@comcast.net
3. **Set Priority and Status:**
   * Set the priority to “Medium.”
   * Set the status to “Assigned.”
4. **Save the Ticket:**
   * Save and submit the ticket for tracking and follow-up.

**Terminology**

**1. DNS Server**

**Overview:**

* A domain controller can also function as a DNS server, which is essential for name resolution within the network.
* When you select this option, the DNS Server role is installed on the domain controller.

**Benefits:**

* Simplifies network management by integrating DNS with Active Directory.
* Ensures that domain controllers can resolve domain names internally.

**2. Global Catalog (GC)**

**Overview:**

* The Global Catalog is a distributed data repository that contains a searchable, partial representation of every object in every domain within a forest.
* A domain controller can be designated as a Global Catalog server.

**Benefits:**

* Facilitates faster searches across the entire forest.
* Provides universal group membership information, which is crucial for logon processes and directory searches.

**3. Read-Only Domain Controller (RODC)**

**Overview:**

* An RODC hosts a read-only copy of the Active Directory database.
* It is designed for use in locations where physical security cannot be guaranteed.

**Benefits:**

* Enhances security by preventing changes to the Active Directory database at the RODC location.
* Reduces the risk of data compromise in less secure environments.

**4. Additional Domain Controller Options**

**Overview:**

* When adding a domain controller to an existing domain, you can configure additional options such as site placement and replication settings.

**Benefits:**

* Allows for better control over replication traffic and site topology.
* Ensures that domain controllers are placed in optimal locations within the network.

**5. FSMO Roles (Flexible Single Master Operations)**

**Overview:**

* FSMO roles are specialized domain controller tasks that are assigned to specific domain controllers to ensure consistency and avoid conflicts.
* There are five FSMO roles: Schema Master, Domain Naming Master, RID Master, PDC Emulator, and Infrastructure Master.

**Benefits:**

* Ensures that certain critical operations are handled by designated domain controllers.
* Helps maintain the integrity and consistency of the Active Directory environment.