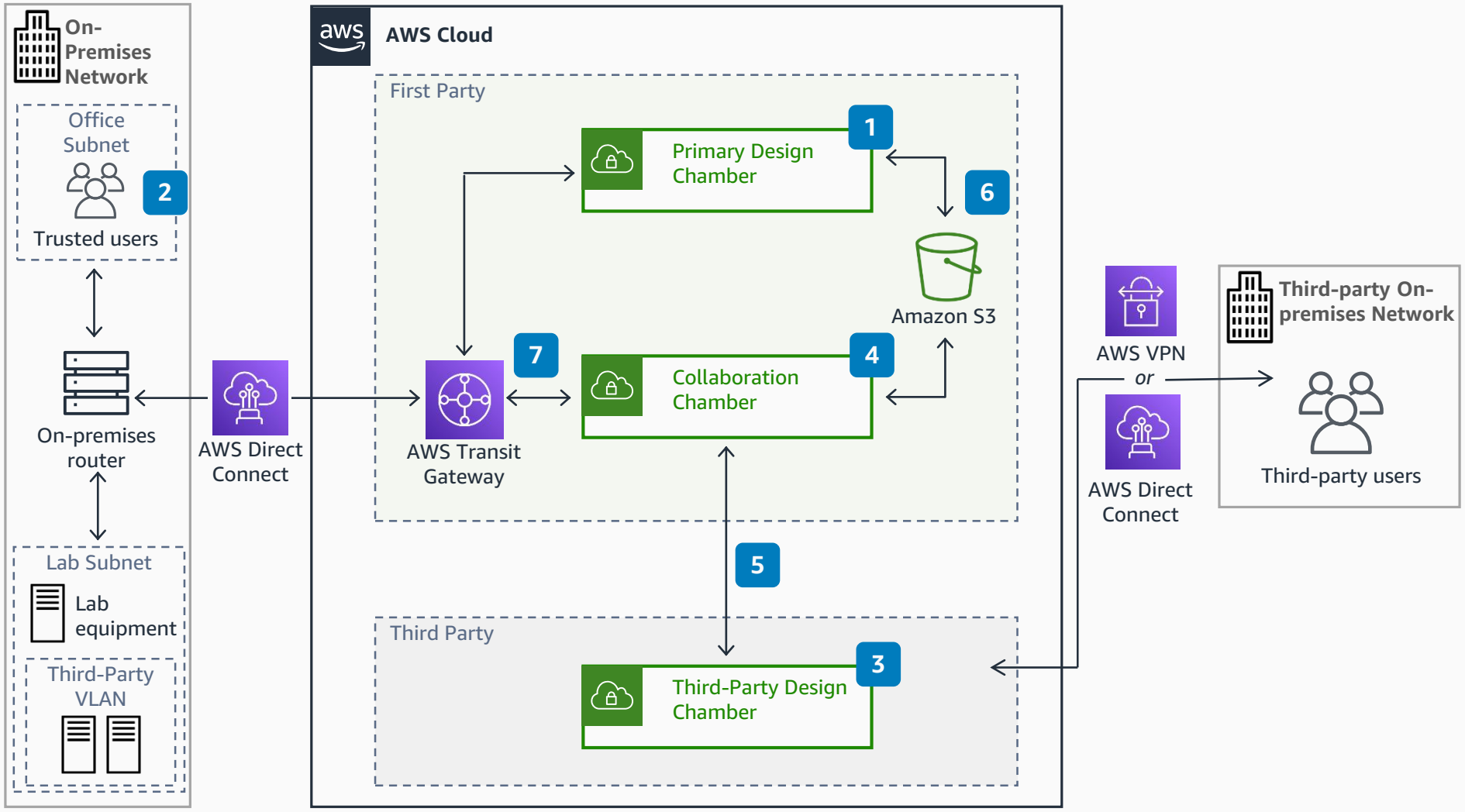
Guidance for Enabling Secure Collaboration on AWS

This architecture enables trusted collaboration with third-party companies for IP design and data exchange in a secure, trusted environment.



1. The basis of a secure collaboration chamber is a primary design chamber built in an **Amazon Virtual Private Cloud (Amazon VPC)**.
2. Trusted users connect to their remote desktops over **AWS Virtual Private Network (AWS VPN)** or **AWS Direct Connect**.
3. Third-party companies develop and test their IP in their own design chambers.
4. To collaborate with third-party companies, create an **Amazon VPC** that will only be used for collaboration with infrastructure based on the primary design chamber. Create accounts, permissions, and remote desktop service endpoints for third-party remote desktops using **AWS PrivateLink**.
5. Third-party companies connect to remote desktops in the collaboration chamber using the service endpoint in their design chamber.
6. Curate data by using **Amazon Simple Storage Service (Amazon S3)** to transfer data in and out of the collaboration chamber. All **Amazon S3** data transfers are logged in **AWS CloudTrail** for auditing. Third-party companies do not have access rights to transfer data out.
7. Third-party users can access on-premises hardware, such as emulators, using routes to an isolated virtual local area network (VLAN) through **AWS Transit Gateway** and **Direct Connect**.
8. When the collaboration is complete, you can delete the collaboration chamber.

Reviewed for technical accuracy April 4, 2023

AWS Reference Architecture