KNOWLEDGE BASE ARTICLE

Firewall Ports for Active Directory Domain Join

The article outlines the essential and optional firewall ports needed for joining an Active Directory domain, including TCP 88 for Kerberos and TCP 135 for RPC. It highlights the importance of opening high TCP ports to avoid RPC server errors.

PUBLISHED
18 Jul 2023

DOCUMENT
InfoHub — Knowledge, news, and updates from EssingtonITS

Firewall Ports for Active Directory Domain Join

18 Jul 2023

Firewall Ports Required to Join an AD Domain (Minimum)

- TCP 88 (Kerberos Key Distribution Centre)
- TCP 135 (Remote Procedure Call)
- TCP 139 (NetBIOS Session Service)
- TCP 389 (LDAP)
- TCP 445 (SMB, Net Logon)
- UDP 53 (DNS)
- UDP 389 (LDAP, DC Locator, Net Logon)
- TCP 49152-65535 (Randomly allocated high TCP ports)

It's crucial to ensure the TCP high ports are open. If they're not, you might run into errors about unavailable RPC servers, which can be a real headache when you're trying to join the domain.

Optional Ports

- UDP 123 (NTP)
- TCP 53 (DNS)
- TCP 464 (Kerberos Password V5 – Used when users change their password from their desktop)
- UDP 137 (NetBIOS Name Resolution)
- UDP 138 (NetBIOS Datagram Service)

- TCP 636 (LDAP SSL)
- UDP 636 (LDAP SSL)
- TCP 3268 (Global Catalogue)