Relazione sulla Configurazione dell’Ambiente Active Directory

Broccoli Gabriele

Stefani Tommaso

Configurazione Domain Controller e Client

Domain Controller:

Domaincontrolle.testenv.local

Indirizzo IP: 192.168.1.24

Risorse della macchina: CPU 4 core, RAM 12 GB, HDD 50 GB

Sistema Operativo: Windows Server 2019

Ruolo: Domain Controller per il dominio testenv.local

Client:

nomeutente.testenv.local

Indirizzo IP: 192.168.1.39

Risorse della macchina: CPU 4 core, RAM 8 GB, HDD 50 GB

Sistema Operativo: Windows 10

Ruolo: Unito al dominio testenv.local

Regole di Firewall generali (in entrata):

Regola 1: Consenti traffico in ingresso sulla porta 53 TCP e UDP (DNS) dal client al domain controller.

Motivo: Necessario per la risoluzione dei nomi di dominio.

Regola 2: Bloccare traffico in ingresso non necessario (porte SMB e NetBIOS) sul domain controller.

Motivo: Ridurre vulnerabilità sul domain controller e aumentare la sicurezza limitando il traffico in ingresso.

Regola 3: Consenti traffico in ingresso sulle porte TCP e UDP 1812

Motivo: Consentire l’autenticazione al server RADIUS

Regola 4: Consenti traffico in ingresso sulle porte 443 e 80

Motivo: Consentire il traffico su protocolli HTTP/HTTPS

Creazione dei Gruppi AD

(Nel progetto reale 2 utenti di esempio per gruppo)

RDP AC Admins:

Ruolo: Amministrazione RDP

Membri: 1

Standard User:

Ruolo: Regole di base per la sicurezza dei client

Membri: Tutti

IT:

Ruolo: Amministrazione IT, gestione della rete e dei server.

Membri: 3

Finance:

Ruolo: Gestione delle finanze aziendali.

Membri: 10

HR:

Ruolo: Gestione delle risorse umane.

Membri: 5

Marketing:

Ruolo: Attività di marketing e pubblicità.

Membri: 15

Sales:

Ruolo: Vendite e relazioni con i clienti.

Membri: 20

Creazione degli Utenti e Assegnazione ai Gruppi

Elenco degli utenti creati e assegnati ai rispettivi gruppi:

RDP AD Admins

TESTENV\erasta

Standard User:

Tutti quelli sotto

IT:

TESTENV\erasta

TESTENV\aesposito

Finance:

TESTENV\clombardi

TESTENV\prusso

HR:

TESTENV\gcaggiano

TESTENV\mstrumolo

Marketing:

TESTENV\amarotta

TESTENV\ivitale

Sales:

TESTENV\pdaniele

TESTENV\rgaetano

Policy di gruppo

Regole di Firewall per gruppo (in entrata)

HR, Finance, Sales, Marketing, IT:

Regola 1:Consenti traffico verso <nome\_reparto>: Permetti (porta 445, SMB)

Motivo: Consentire comunicazione interna al reparto

Regola 2: Allow DNS TCP: Permetti (porta 53, TCP)

Motivo: DNS

Regola 3: Allow DNS UDP: Permetti (porta 53, UDP)

Motivo: DNS

Regola 4: Allow Kerberos: Permetti (porta 88, TCP)

Motivo: Consentire autenticazione Kerberos

Regola 5: Allow LDAP: Permetti (porta 389, TCP)

Motivo: Consentire autenticazione LDAP

Regola 6: Default Deny: Blocca

Motivo: Blocca tutto il resto

RDP DC Admins:

le stesse regole sopra, e in aggiunta

Regola 7: Consenti traffico RDP: Permetti (porta 3389, TCP, attivo)

Motivo: Consenti la connessione Remote Desktop

Applicazione delle GPO

Standard User:

Policy Computer -> Security Settings -> Policy di Sicurezza Account:

GPO 1: Maximum Password Age: 90 giorni

GPO 2: Minimum Password Age: 0 giorni

GPO 3: Minimum Password Length: 4 caratteri

Scopo: Fornire un set di regole base per la creazione di account sicuri

RDP DC Admins:

GPO 1:Consentire la connessione remota tramite Servizi Desktop remoto: Abilitato

Scopo: Consente agli utenti di connettersi al computer di destinazione tramite Servizi Desktop remoto.

IT:

GPO 1:Seleziona quando ricevere le build di anteprima e gli aggiornamenti delle funzionalità: Abilitato

GPO 2:Livello di disponibilità: Canale semestrale

GPO 3:Rinvio degli aggiornamenti: 0 giorni

Scopo: lasciare meno libertà agli utenti sugli aggiornamenti, obbligatorio aggiornamento semestrale alla ultima build stabile.

Finance, HR, Marketing, Sales:

GPO 1: Impedisci l'accesso al Pannello di controllo e a Impostazioni PC: Abilitato

Scopo: Impedisce l'accesso al Pannello di controllo e Impostazioni PC.

Creazione delle Share di Rete/ACL

Sul Domaincontroller --> C:/Shared

IT:

Percorso: \\DomainControlle\IT

ACL: Accesso completo solo al gruppo IT.

Finance:

Percorso: \\DomainControlle\Finance

ACL: Accesso completo solo al gruppo Finance.

HR:

Percorso: \\DomainControlle\HR

ACL: Accesso completo solo al gruppo HR.

Marketing:

Percorso: \\DomainControlle\Marketing

ACL: Accesso completo solo al gruppo Marketing.

Sales:

Percorso: \\DomainControlle\Sales

ACL: Accesso completo solo al gruppo Sales.

Controllo degli Accessi RDP

Accesso RDP limitato all’amministratore Enzo Rasta (TESTENV\erasta), unico membro del gruppo RDP DC Admins, da IP del client.

Firewall configurato per aprire porta RDP solo agli utenti del gruppo RDP DC Admins.

Configurazione di un Server RADIUS

* Installazione del ruolo Network Policy Server (NPS/NPAS) tramite Server Manager.
* Registrazione del server NPS nel dominio.
* Aggiunta di un client RADIUS (Test Client) con indirizzo IP 192.168.1.39 e chiave condivisa.

Policy di Accesso RADIUS

Policy 1: Consentire l'accesso alla rete a tutti gli utenti autenticati.

Policy 2: Consentire l'accesso alla rete amministrativa solo agli utenti del gruppo Domain Admins.

Conclusione

Il progetto di configurazione dell'ambiente Active Directory è stato fatto implementando le misure di sicurezza necessarie per proteggere l'infrastruttura.

Le regole firewall, le ACL e le policy di accesso sono state configurate per garantire un ambiente ben gestito e organizzato. L'installazione del server RADIUS aggiunge un ulteriore livello di sicurezza per l'autenticazione della rete.