Förarbete

Vilka är vi?

BrewIT är ett nystartat företag grundat av två entusiaster med inriktning på att bygga IT-miljöer. Med bred kompetens inom serverhantering och nätverkslösningar levererar vi skräddarsydda, säkra och kostnadseffektiva lösningar som möter våra kunders behov.

Tillsammans med oss får ni en IT-miljö som inte bara är robust och pålitlig, utan också anpassad för framtidens behov.

Erbjudande

I enlighet med vår tidigare dialog presenterar BrewIT härmed ett erbjudande för att utforma och implementera er nya IT-miljö i linje med era specifika krav.

Behov/Önskemål

DesignDreamers har specificerat följande behov och önskemål för sin framtida IT-miljö:

- **Central identiteshantering:** En lösning för att hantera användaridentiteter och autentisering på ett centraliserat och säkert sätt.
- **Behålla befintliga Linux-datorer:** Deras nuvarande Linux-baserade arbetsstationer ska fortsätta användas som en del av den nya miljön.
- **Möjlighet att använda Windows-datorer:** Flexibilitet att lägga till och använda Windows-datorer i IT-miljön.
- **Kostnadseffektivitet:** Maximal återanvändning av befintlig IT-utrustning för att hålla kostnaderna nere.

Nuläge

DesignDreamers nuvarande IT-miljö består av:

1. Tre Linuxbaserade arbetsstationer.
2. Två Linuxbaserade servrar.
    - Databasserver – Hanterar data för WordPress
    - Webbserver – Presentation av designer.
3. En Technicolor TG799vac Xtream router med begränsade konfigurationsmöjligheter.

De har förberett ett nytt kontor i Solna med tillräckligt utrymme för alla anställda. Kontoret är redo att stödja verksamheten och tillväxten framöver. Det är utrustat med en snabb fiberanslutning på 250/250 Mbit.

Vår lösning

För att optimera befintliga resurser och skapa en skalbar IT-miljö föreslår BrewIT följande lösning:

1. **Virtualisering av befintliga servrar:**
   De två nuvarande fysiska servrarna kommer att delas upp i fyra stycken virtuella servrar, vilket möjliggör flera servrar på samma hårdvara med olika operativsystem. Detta maximerar nyttjandet av befintliga resurser och minskar behovet av nya inköp.
2. **Integration av Linux-klienter:**
   Användare med Linux-datorer kan fortsätta arbeta med sina nuvarande enheter, men övergår till centralt administrerade användarkonton. Vi tillhandahåller en lösning för att ansluta Linux-datorerna till företagets interna nätverk för att förbättra säkerhet och kontroll.
3. **Förbättrad nätverkssäkerhet:**
   För att skydda företagets interna miljö och webbservern mot externa hot införskaffas en router med inbyggd brandvägg och ett extra nätverkskort till webbservern. Dessa åtgärder kommer att säkerställa att den är logiskt åtskild från företagets övriga nätverk.
4. **Licenshantering av Linux-klienter:**
   För att möjliggöra central administration av Linux-klienter behöver dessa utrustas med en Ubuntu Pro-prenumerationslicens, vilket även inkluderar säkerhets- och kompatibilitetsuppdateringar.
5. **Windows-domän:**
   Två servrar med Windows Server-operativsystem konfigureras för att skapa en domän, vilket möjliggör centraliserad hantering av användare och resurser.
6. **Windows Server och licenshantering:**
   De fysiska servrarna kommer att använda Windows Server Standard som operativsystem. Valet av Windows motiveras av att några av de virtuella servrarna ändå kräver Windows-licens, och en standardlicens inkluderar licenser för dessa också; vilket gör detta till en kostnadseffektiv och praktisk lösning.

Utöver detta behöver varje klient som ansluter till Windows Server en **Client Access License (CAL)**, vilket säkerställer korrekt licensiering för klienternas åtkomst till servern.

Denna lösning kombinerar återbruk, kostnadseffektivitet och förbättrad säkerhet.

Teknisk specifikation

DesignDreamers erbjuds en säker och robust IT-miljö som omfattar två domänkontrollanter som kontinuerligt replikerar mellan varandra för att säkerställa hög tillgänglighet och felsäkerhet. Lösningen inkluderar också en databasserver för att hantera WordPress-data.

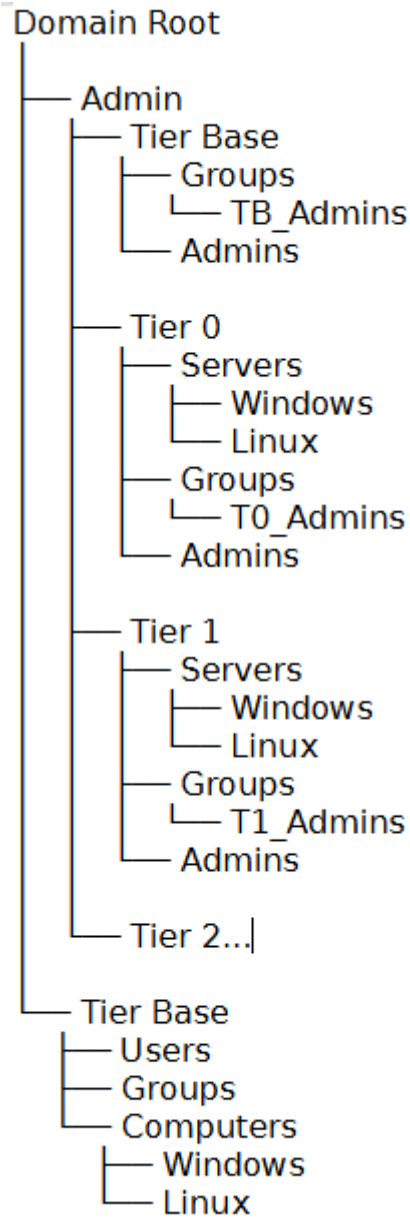
Webbservern med WordPress är placerad i en DMZ (Demilitarized Zone) för att isolera den från företagets interna nätverk. För att komplettera säkerheten installeras en brandvägg för att motverka intrång och skydda hela företagets IT-miljö.

Serverkonfiguration:

- **Server 1:**
  - Operativsystem: Windows Server 2022 Standard
  - Virtuella maskiner:
    - VM1: Domänkontrollant 1 – Windows Server 2022 Standard
    - VM2: Databasserver – Ubuntu Server 24.04 LTS

- **Server 2:**
  - Virtuella maskiner:
    - VM1: Domänkontrollant 2 – Windows Server 2022 Standard
    - VM2: Webbserver – Ubuntu Server 24.04 LTS
  - Extra: Nätverkskort för DMZ-konfiguration

- **Router:** Ubiquiti Cloud Gateway Ultra
- **Switch:** TP-Link TP-SG116, 16P omanagerad gigabit switch.



AD-Struktur:

Varje tier har dedikerade administratörskonton som är strikt isolerade från att logga in på resurser i andra tiers, vilket minskar risken för spridning av potentiella hot.

- **Tier 0: Kritiska resurser**
  - **Innehåll:** Domänkontrollanter och andra affärskritiska resurser.
  - **Administratörsroller:** Tier 0-administratörer har fullständig kontroll över domänen och hanterar resurser som utgör kärnan i IT-miljön. Dessa konton har den högsta nivån av säkerhet och åtkomstbegränsningar.
- **Tier 1: Applikations- och dataservrar**
  - **Innehåll:** WordPress-servern och databasservern.
  - **Administratörsroller:** Tier 1-administratörer hanterar specifikt dessa servrar, inklusive administration av applikationer, databaser och innehåll, utan åtkomst till Tier 0-resurser.
- **Tier Base: Användare och klienter**
  - **Innehåll:** Användarkonton och klienter.
  - **Administratörsroller:** Administratörer i Tier Base ansvarar för användarhantering, inklusive grupptillhörighet, lösenordshantering samt skapande och borttagning av användarkonton. De har endast åtkomst till resurser och enheter i denna tier.

Nätverk:

En ny router med avancerade brandväggsfunktioner införskaffas, och WordPress-servern placeras i ett dedikerat DMZ för att isolera servern från det interna nätverket.

På routern implementeras routing- och brandväggsregler för att säkerställa att nätverkstrafiken styrs effektivt mellan segmenten och att endast behörig åtkomst tillåts.

WordPress:

WordPress-servern hanteras av Tier 1-administratörer, som har full tillgång till serverns operativsystem samt administratörsbehörighet inom WordPress-applikationen.

För att integrera WordPress med företagets Active Directory används tillägget Next Active Directory Integration.

Script:

Vid överlämning tillhandahåller vi vissa skripts som är användbara för löpande drift.

Dessa inkluderar:

- **Användarimport:**
  Script för att importera användare från en fördefinierad CSV-fil direkt till Active Directory.
- **Linux-klientkonfiguration:**
  Script för att konfigurera Linux-klienter att ansluta till domänen med hjälp av realmd och sssd.

För Linux-klienter krävs en Ubuntu Pro-licens för att möjliggöra tillämpning av GPO:er från Active Directory.

Utöver scripten lämnar vi också över en utförlig teknisk dokumentation som beskriver hur IT-miljön är konfigurerad. Dokumentationen fungerar som en guide för att förstå och underhålla infrastrukturen, och ger DesignDreamers möjlighet att bygga vidare på miljön och anpassa den efter framtida behov.