Agenda Workshop Endpoint Management

1 Einleitung

In einem gemeinsamen Workshop werden durch AN in Zusammenarbeit mit dem AG folgende Tasks ausgearbeitet, um die Integration eine Mobile Device Management Lösung zu planen und umzusetzen.

2 Workshop - Enrollment

2.1 Ermitteln der Eckdaten des AG

- Betriebsgröße (Anzahl der Mitarbeiter)
- Anzahl der Standorte
- Definieren der Ziele für den Workshop

2.2 Analyse

- Welche Use-Cases sollen abgebildet werden?
    - Welches sind die größten Herausforderungen bei der Geräteverwaltung, mit denen Sie konfrontiert sind?
    - Stellt Ihr Unternehmen den Mitarbeitern Firmenhandys und/oder Tablets zur Verfügung?
    - Dürfen Mitarbeiter von privaten Telefonen oder Tablets aus auf E-Mails, Daten oder Anwendungen des Unternehmens zugreifen?
    - Haben die Mitarbeiter von ihrem firmeneigenen Windows-Laptop aus Fernzugriff auf Unternehmensanwendungen und -daten?
- Aktueller Stand Microsoft 365
    - Welche Art und Anzahl von Lizenzen besitzen Sie derzeit?
    - Welche Microsoft 365-Dienste haben Sie im Einsatz?
    - Welche Azure-Dienste haben Sie eingesetzt?
    - Welche Geräte wurden für Microsoft 365 oder Azure-Dienste aktiviert?
- Device Management
    - Welche Mobile Device Management (MDM)-Lösungen haben Sie derzeit im Einsatz, wenn überhaupt?
    - Werden Windows 10- oder 11-Geräte derzeit mit Microsoft Endpoint Configuration Manager verwaltet?
    - Kann Ihr IT-Team alle Arbeitsgeräte über eine einzige Konsole verwalten?
    - Kann die IT-Abteilung Unternehmensdaten in verwalteten Apps (einschließlich Office Mobile-Apps) schützen, die auf privaten Geräten verwendet werden, einschließlich der Geräte von Mitarbeitern, die nicht von der IT-Abteilung verwaltet werden?
    - In welchem Besitz befinden sich die Geräte, die Sie mit einer MDM-Lösung verwalten möchten?
    - Welche Arten von Geräten möchten Sie mit einer MDM-Lösung verwalten?
    - An welchen MDM-Funktionen sind Sie besonders interessiert?
    - Verfügt Ihr Unternehmen über ein Android Enterprise-Konto zur Verwaltung von Android-Geräten?

2.3 Infrastruktur (Möglichkeiten/Abhängigkeiten)

- Endpoint Manager/Intune standalone (Cloud-only)
    - Mobile Geräte
- Co-Management

    - Zusätzlich zu mobilen Geräten werden Windows PCs, Windows Server, Linux Server und macOS unterstützt
    - Verwaltung disloziert (Cloud und on-Premise)
    - Für die gemeinsame Verwaltung ist Configuration Manager Version 1710 oder höher erforderlich.
- Tenant attached
    - Ab der Version 2002 von Configuration Manager können Sie Ihre Configuration Manager-Geräte in den Cloud-Service hochladen und über das Blade "Geräte" im Verwaltungszentrum Aktionen durchführen
    - Zusätzlich zu mobilen Geräten werden Windows PCs, Windows Server, Linux Server und macOS unterstützt

2.4 Festlegung der Identitätsverwaltung

- Cloud Identität
    - Vorteile:
        - Kann für kleine Organisationen einfacher zu verwalten sein.
        - Es muss nichts vor Ort installiert werden.
        - Keine zusätzliche Hardware erforderlich.
        - Leichte Deaktivierung, wenn der Benutzer das Unternehmen verlässt.
    - Nachteile:
        - Zusätzlicher Aufwand für die Erstellung von Cloud-Identitäten.
        - Die Benutzer müssen sich anmelden, wenn sie auf Workloads in der Cloud zugreifen.
        - Passwörter können für Cloud- und lokale Identitäten identisch sein oder auch nicht.
        - Erfordert zusätzlichen Aufwand für die Migration von Cloud-Identitäten zu synchronisierten Identitäten
- Synchronisierte Identität
    - Vorteile:
        - Vor-Ort-Passwort authentifiziert sowohl vor Ort als auch in der Cloud.
        - Kann für kleine, mittlere oder große Organisationen einfacher zu verwalten sein.
        - Benutzer können sich für einige Ressourcen einzeln anmelden (SSO).
        - Von Microsoft bevorzugte Methode für die Synchronisierung
        - Leichter zu verwalten.
    - Nachteile:
        - Einige Kunden zögern möglicherweise, ihre Verzeichnisse mit der Cloud zu synchronisieren, weil sie bestimmte Unternehmensrichtlinien haben.
- Föderierte Identität
    - Vorteile:
        - Benutzer können sich einmalig anmelden (SSO).
        - Wenn ein Benutzer gekündigt wird oder ausscheidet, kann das Konto sofort deaktiviert und der Zugriff widerrufen werden.
        - Unterstützt erweiterte Szenarien, die mit synchronisiert nicht möglich sind.
    - Nachteile:
        - Mehr Schritte zum Einrichten und Konfigurieren.
        - Höherer Wartungsaufwand.

- Erfordert zusätzliche Hardware.
- Erfordert eine umfangreiche Einrichtung für SSO.
- Kritischer Fehlerpunkt, wenn der Föderationsserver ausfällt und die Benutzer sich nicht authentifizieren können.

2.5 Enrollment Methoden

- Windows
  - GPO
  - Co-management
  - Device Enrollment Manager
- iOS
  - Apps verwaltet
  - User Registrierung (Unternehmensportal) / BYOD
  - Auto-Registrierung (ABM)
- Android
  - Apps verwaltet
  - User Registrierung (Unternehmensportal) / BYOD
  - Unternehmensgerät mit Arbeitsprofil
  - Unternehmensgerät Full managed
  - Unternehmensgerät spezifischer Einsatz

3 Workshop - Konfiguration

3.1 Überblick der Konfigurationsmöglichkeiten

- Device Features
  - Steuert Funktionen des Geräts (Beispiele: Airprint, Benachrichtigungen und Sperrbildschirm-Nachrichten)
- Device restrictions
  - Steuert Sicherheit, Hardware, Datenfreigabe und weitere Einstellungen auf den Geräten (Beispiele: Erfordernis einer PIN, Datenverschlüsselung usw.)
- Access configuration
  - Bereitstellung der Zugangskonfiguration der Organisation für das Gerät (Beispiele: E-Mail-Profile, VPN-Profile, Wi-Fi-Einstellungen, Zertifikate usw.
- Custom
  - Festlegen einer benutzerdefinierten Konfiguration oder Ausführen benutzerdefinierter Konfigurationsaktionen (Beispiele: OEM-Einstellungen festlegen, PowerShell-Skripte ausführen usw.)

3.2 Zuweisung von Konfigurationen

- Konfigurationsprofile können Benutzergruppen oder Gerätegruppen zugewiesen werden
  - Verwenden von Benutzergruppen. Einstellungen und Regeln gelten immer für den Benutzer, unabhängig davon, welches Gerät verwendet wird.
  - Verwenden von Gerätegruppen, wenn es egal ist, wer sich auf dem Gerät anmeldet oder ob sich jemand anmeldet. Einstellungen immer auf dem Gerät
  - Ein Gerät muss von Intune verwaltet werden, damit Konfigurationsprofile zugewiesen werden können.

        - Einem Benutzer oder Gerät können ein oder mehrere Konfigurationsprofile zugewiesen werden.
- Verwenden von Gruppen für Ausschlüsse, um Benutzer oder Geräte von der Profilzuweisung auszuschließen.
    - Der Ausschluss hat in Szenarien mit demselben Gruppentyp Vorrang vor dem Einschluss
    - Benutzergruppen einschließen und Benutzergruppen ausschließen
    - Einschluss von Gerätegruppen und Ausschluss von Gerätegruppen
    - Beim Mischen von Gruppentypen (z. B. einschl. Benutzergruppe und ausschl. Gerätegruppe) hat die Einbeziehung Vorrang.
- Benutzung von Filtern
    - Ermöglicht Administratoren die Aufnahme oder den Ausschluss von Geräten in eine Gruppe auf der Grundlage vom Administrator festgelegter Kriterien
    - Zuweisungsfilter ermöglichen es, eine Abfrage über Geräteeigenschaften für eine Betriebssystemplattform zu definieren.
    - Ein Filter kann in mehreren Szenarien als wiederverwendbare Einheit verwendet werden
- Unterstützte Geräteeigenschaften
    - Hersteller
    - Modell
    - Gerätekategorie
    - OS-Version
    - IsRooted
    - Eigentum am Gerät
    - Name des Enrollment-Profils
    - SKU des Betriebssystems (Windows 10)
- Profilzuweisung
    - Online
        - Alle 8 Stunden
    - Offline
        - Beim nächsten geplanten Check-in, wenn das Gerät online ist
    - Gerät ist online und Konfigurationsprofil wurde zugewiesen oder geändert
        - Intune benachrichtigt das Gerät, um das Profil abzurufen. Die Benachrichtigungszeit variiert von sofort bis zu ein paar Stunden
    - Gerät ist offline und Konfigurationsprofil wurde zugewiesen oder geändert
        - Intune versucht bis zu vier Mal, das Gerät zu benachrichtigen. Wenn das Gerät nicht antwortet, erhält es beim nächsten geplanten Einchecken ein aktualisiertes Konfigurationsprofil.
- Umgang mit Konflikten
    - Die Einstellungen der Compliance-Richtlinie haben immer Vorrang vor den Einstellungen des Konfigurationsprofils.
    - Wenn eine Konformitätsrichtlinie gegen dieselbe Einstellung in einer anderen Konformitätsrichtlinie bewertet wird, gilt die restriktivste Einstellung der Konformitätsrichtlinie.
    - Wenn eine Konfigurationsrichtlinieneinstellung mit einer Einstellung in einer anderen Konfigurationsrichtlinie in Konflikt steht, wird dieser Konflikt in Intune angezeigt. Lösen Sie diese Konflikte manuell auf.

3.3 Erstellen der Profile

- Security Baselines
  - Beginnen mit Sicherheits-Baselines - die von Microsoft empfohlene Best-Practice-Konfiguration
- Individuelle Einstellungen
  - Füllen von Konfigurationslücken mit individuellen Einstellungen in Gerätekonfigurationsprofilen oder aus dem Einstellungskatalog
- ADMX Templates
  - Erfüllen von älteren Konfigurationsanforderungen mit administrativen (ADMX) Vorlageneinstellungen
- Geräte Complianceeinstellungen
  - Sicherstellen, dass die Geräte und Benutzer die IT-Richtlinien einhalten

3.4 Security Baselines

- Sicherheits-Baselines sind vorkonfigurierte Gruppen von Windows-Einstellungen und Standardwerten, die von den zuständigen Microsoft-Sicherheitsteams empfohlen werden
- Ein Sicherheits-Baseline-Profil ist eine Vorlage, die aus mehreren Gerätekonfigurationsprofilen besteht.

Vorteile

- Enthält die besten Praktiken und Empfehlungen für Einstellungen, die sich auf die Sicherheit auswirken
- Ein guter Ausgangspunkt für die schnelle Erstellung und Bereitstellung eines sicheren Konfigurationsprofils
- Erleichtert die Migration von der Gruppenrichtlinie zur Intune-Verwaltung

3.5 ADMX Templates

- Administrative Vorlagen enthalten Tausende von Einstellungen, die Funktionen in Microsoft Edge Version 77 und höher, Microsoft Office-Programmen, Remotedesktop, OneDrive, Kennwörtern, PINs und mehr steuern
- Administrative Vorlagen enthalten ADMX-gestützte Windows-Einstellungen, die mit den Gruppenrichtlinieneinstellungen in Active Directory vergleichbar sind.

Vorteile

- Administrative Vorlagen sind in Intune integriert und erfordern keine Anpassungen
- Die zentrale Anlaufstelle für die Verwaltung Ihrer Windows 10-Geräte
- Erleichtert die Migration von der Gruppenrichtlinie zur Intune-Verwaltung

3.6 Custom Settings

- Verwenden Sie benutzerdefinierte Profile, um Geräteeinstellungen und Funktionen zu nutzen, die nicht in Intune integriert sind.
- Benutzerdefinierte Einstellungen werden für jede Plattform unterschiedlich konfiguriert und werden unterstützt von
  - Android DA und Enterprise
  - iOS/iPadOS
  - macOS
  - Windows 10/11 und Windows Holographic for Business

3.7 Migration bestehender GPOs

- Export der GPS als XML
- Import XML in Intune
- Intune analysiert die GPOs und verknüpft die Einstellung zu den Intune-Einstellungen
- Ausrollen der CSPs und Ergänzen fehlender Einstellungen mit angepassten URI

3.8 Application lifecycle management

- Add
  - Viele Anwendungstypen sind verfügbar, darunter Store-, Web- oder LOB-Anwendungen (intern)Deploy
- Deploy
  - Einfache Bereitstellung durch Gruppen mit Einschluss-/Ausschluss- und Filteroptionen, Überwachung ist möglichConfigure
- Configure
  - Konfigurieren von Anwendungseinstellungen und Aktualisieren neuer Versionen
- Protect
  - Schutzverhalten, Zugangskontrolle, Compliance-Richtlinien
- Retire
  - Intune bietet einfache Schritte zum Entfernen von Zuweisungen oder zum Zurückziehen von Geräten und ihren Anwendungen
- Supported App Types
- App Assignment

3.9 Store Integration

- Microsoft Store for Business
  - Verwenden Sie den privaten Store
  - Zuweisung von Anwendungslizenzen direkt an Benutzer
  - Integration mit Verwaltungstools

4 Protection

4.1 Multifaktor Authentifizierung

- Cloud Only
  - Keine weiteren Voraussetzungen
- Hybrididentity
  - Azure AD Connect zur Synchronisierung von Identitäten und/oder im Verbund mit On-Premises AD DS
- Veröffentlichung von Legacy-Anwendungen vor Ort für den Zugriff auf die Cloud
  - Azure AD Application Proxy
- Azure MFA mit RADIUS-Authentifizierung (On-Prem-Apps)
  - Netzwerkrichtlinienserver mit installiertem MFA-Adapter

4.1.1 Azure MFA Einrichtung

- Conditional access
  - Die vielseitigste Art, MFA zu ermöglichen. Empfohlener Ansatz

- Security defaults
    - Ermöglicht MFA für alle Benutzer. Empfohlen vor allem für kleine Unternehmen bei sorgfältiger Abwägung
- Per-user account
    - Herkömmliche Methode zur Aktivierung von MFA. Nicht empfohlen

4.1.2 Azure MFA mit Conditional access

- Azure MFA wird durch Richtlinien für den bedingten Zugriff aktiviert, die während des Anmeldevorgangs angewendet werden auf
    - Alle oder ausgewählte Gruppen von Benutzern
    - Alle oder eine beliebige Cloud-Anwendung
- Die Anforderungen für Azure MFA können auch auf folgenden Kriterien basieren
    - Standort
    - Art der Cloud-Anwendung
    - Echtzeit-Risiko (erfordert AAD P2-Lizenz)
    - Gerätestatus (erfordert Intune-Lizenz)
- Benutzerregistrierung für zweiten Faktor bei der nächsten Anmeldung nach Aktivierung der Richtlinie für bedingten Zugriff (Erfordert Azure Active Directory Premium P1-Lizenz). Oder eine Lizenz, die sowohl MFA als auch Conditional Access beinhaltet, wie
    - Azure Active Directory Premium P2,
    - Microsoft 365 Business,
    - Microsoft 365 E3
    - Microsoft 365 E5
- Azure MFA zweiter Faktor
    - SMS, Anruf, Push, One Time Passcode, Hardtoken OTP, Softtoken OTP, FIDO2
- Microsoft Authenticator App
    - Multi-Account-fähig
    - Benachrichtigungen mit einfacher Freigabe/Ablehnung
    - Einmaliger Passcode mit einfachem Klick zum Kopieren für Benutzerfreundlichkeit
    - Benachrichtigung mit zweistelligem Verifizierungscode für vollständige telefonische Anmeldung

4.2 Azure AD Password Protection

- Smart Lockout zum Verhindern des Erratens von Passwörtern durch böswillige Akteure
- Dynamisches Verbot von Passwörtern auf der Grundlage bekannter und von Ihnen definierter schlechter Muster
- Entwickelt für hybride Umgebungen
- Einheitliche Verwaltungserfahrung für On-Premises und Cloud

Verbotene Passwörter in Azure AD werden auf lokales Windows Server Active Directory ausgeweitet

Ziele:

- Stärkung der hybriden Azure AD-Umgebung vor Ort
- Nutzung der Azure-basierten Passwortschutzlogik
- Einfache, leicht zu verwaltende und skalierbare Bereitstellung von sicheren, leichtgewichtigen Agenten

- Funktioniert mit bestehenden Windows Server AD-Implementierungen über mehrere Forests hinweg

Self-service password reset (SSPR) für Clouly only users or AD User mit Passwort writeback

- Passwortvergabe und Passwortreset
- Passwortwechsel
- Passwort writeback
- Account unlock

4.3 Windows Hello for Business

- Benutzerfreundlich
  - Kein Passwort erforderlich
  - Biometrie oder eine PIN
  - SSO mit Windows-Anwendungen über Web Account Manager (SSO) APIs
- Unternehmenstauglich
  - Starke Zwei-Faktoren-Authentifizierung
  - Asymmetrisches Schlüsselpaar-Authentifizierungsmodell
  - Kann in Cloud-, Hybrid- oder lokalen Umgebungen eingesetzt werden
  - Mehrere Konten werden unterstützt
- PIN Windows Hello
- Fingerabdruck Windows Hello
- Gesichtserkennung Windows Hello
  +
- Zertifikate Windows Hello for Business
- Security Keys Windows Hello for Business

4.3.1 WHfB Rollout

Microsoft Endpoint Manager (MEM) lässt sich auf zwei Arten mit WHfB integrieren

Tenant-weit: eine WHfB-Richtlinie unter Geräteregistrierung: wird angewendet, wenn das Gerät registriert wird.

Einzelne Gruppen: eine Gerätekonfiguration Identitätsschutzprofil für Geräte, die sich zuvor bei Intune angemeldet haben, wird beim Einchecken des Geräts angewendet.

Zusätzlich unterstützt MEM den folgenden Richtlinientyp, um einige Einstellungen für WHfB zu verwalten

- Sicherheits-Basislinien
- Endpunktsicherheit Kontoschutz

4.4 Endpoint Security

Microsoft Endpoint Manager (MEM) bietet Sicherheitsrichtlinien für Endgeräte, d. h. eng gefasste Sicherheitseinstellungen auf Geräteebene, die die Konfiguration von:

- Antivirus, Festplattenverschlüsselung, Firewalls
- Mehrere Bereiche werden durch die Integration mit Microsoft Defender for Endpoint verfügbar gemacht

Mit Endpunktsicherheitsrichtlinien kann die Gerätesicherheit konfiguriert werden, ohne dass der Overhead für die Navigation durch den größeren Bereich von Einstellungen in Gerätekonfigurationsprofilen und Sicherheits-Baselines entsteht

Endpunkt-Sicherheitsrichtlinien können angewendet werden auf:

- Windows-Geräte
- macOS-Geräte

Was wird angeboten?

- Firewall settings
- Account Protection settings
- Disk encryption
- Defender Endpoint settings

4.5 Appschutzrichtlinien

Microsoft Endpoint Manager (MEM) bietet App-Schutzrichtlinien (APP), d. h. Regeln auf App-Ebene, die die Unternehmensdaten Ihres Unternehmens verwalten und schützen können.

- App-Schutzrichtlinien können angewendet werden auf
  - iOS/iPadOS-Geräte (iPhones, iPads, iPods)*
  - Android-Geräte
  - Windows-Geräte
- Welche Möglichkeiten gibt es
  - Multi-Identität Awareness
  - Datensicherheit
  - Zugangsvoraussetzungen
  - Startbedinungen
- App-Schutzrichtlinien für nicht verwaltete Geräte
  - App-Schutzrichtlinien (APP) können auf nicht verwalteten Geräten zum Schutz ausgewählter öffentlicher Anwendungen* oder Line-of-Business (LoB)-Anwendungen** eingesetzt werden.
  - App-Schutzrichtlinien werden vom MEM Intune Mobile Application Management (MAM)-Dienst bereitgestellt

Was wird angeboten?

- Datensicherheit
- Auditberichte
- Datentrennung
- WIPE Möglichkeiten