KAPITEL 1

Moderne Gerätedienste implementieren

Dieses Kapitel befasst sich mit cloudbasierten Diensten innerhalb von Microsoft 365, die für die Bereitstellung, die Absicherung und die Verwaltung von Geräten im Unternehmen entworfen wurden. Im Laufe dieses Buches werden Sie mit verschiedenen Microsoft-Technologien arbeiten, die in der Enterprise Mobility + Security (EMS)-Lizenzierungssuite enthalten sind. Ein Großteil der Dienste wird über das Microsoft Endpoint Manager Admin Center verwaltet, aber es gibt auch weitere Portale wie das Azure Portal und das Portal Microsoft Store für Unternehmen. Im Laufe des Kurses werden mehrere Beispiele und Komplettlösungen vorgestellt, die die Verwaltung dieser Tools veranschaulichen. Für die Demonstrationen empfehlen wir, dass Sie diese in Ihrem eigenen Labor nachzuvollziehen. Hier finden Sie einige Links, die Ihnen den Einstieg erleichtern:

- **Enterprise Mobility + Security 90-Tage-Testversion (enthält Azure Active Directory Premium P2)** ***https://www.microsoft.com/cloud-platform/enterprise-mobility-security-trial***
- **Office 365 Business Premium 30-Tage-Testversion** ***https://products.office.com/business/office-365-business-premium***

In diesem Kapitel abgedeckte Prüfungsziele:

- Prüfungsziel 1.1: Planung der Geräteverwaltung
- Prüfungsziel 1.2: Verwaltung der Gerätekonformität
- Prüfungsziel 1.3: Planung von Apps
- Prüfungsziel 1.4: Planung der Windows 10-Bereitstellung
- Prüfungsziel 1.5: Registrierung von Geräten

Prüfungsziel 1.1: Planung der Geräteverwaltung

Die Geräteverwaltung ist einer der Kerndienste von Microsoft Intune, der über das Microsoft Endpoint Manager Admin Center verwaltet wird. Die Geräteverwaltung setzt voraus, dass der Microsoft Endpoint Manager konfiguriert ist und dass im Mandanten die entsprechenden Lizenzen verfügbar sind. Sie weisen diese Lizenzen den Benutzern zu, die wiederum die im Mandanten registrierten Geräte verwenden können. Nachdem die Geräte registriert sind, können Sie diese über das Microsoft Endpoint Manager Admin Center verwalten und überwachen.

Dieser Abschnitt behandelt die folgenden Themen:

- Planen der Geräteüberwachung
- Planung der Implementierung von Microsoft Endpoint Manager
- Planung von Konfigurationsprofilen

Planen der Geräteüberwachung

In diesem Abschnitt werden die Optionen für die Geräte- oder Endpunktüberwachung in Microsoft 365 Defender vorgestellt. Diese Angebote ermöglichen es Unternehmen, den Zustand und die Compliance der Geräte und Anwendungen in ihrer Umgebung zu überwachen. Die beiden wichtigsten Tools für die Überwachung von Endpunkten werden über das Microsoft 365 Security Center und das Microsoft Endpoint Manager Admin Center bereitgestellt.

Das Microsoft 365 Security Center ist eine zentrale Anlaufstelle, die Defender für Endpunkt, Defender for Office 365, Microsoft 365 Defender und andere Tools in einer Oberfläche zusammenfasst.

Über das Security Center können Sie viele Überwachungsaktionen durchführen:

- **Anzeigen Ihrer Microsoft-Sicherheitsbewertung** Die Sicherheitsbewertung empfiehlt Ihnen auf der Grundlage der aktuellen Konfiguration Ihrer Umgebung Verbesserungsmaßnahmen.
- **Anzeigen der Gerätekonformität** Bestimmen Sie die Anzahl, den Typ und die Namen der Geräte, die konform sind, nicht konform sind, sich in einer Toleranzperiode befinden oder nicht bewertet werden.
- **Anzeigen der gefährdeten Geräte** Zeigen Sie die Anzahl der Geräte und deren Risikostufe auf der Grundlage der aktuellen Konfiguration an.
- **Geräte mit aktiver Malware anzeigen** Verfolgen Sie die Sicherheitsereignisse und erzwingen Sie die Konfiguration, Konformität und Behebung über die Intune-Geräteverwaltung.

Um Microsoft 365 Defender zu aktivieren, müssen Sie entweder die Rolle des globalen Administrators oder des Sicherheitsadministrators von Azure Active Directory haben. Wenn Sie Microsoft 365 Defender aktivieren, müssen einige Einstellungen für den Mandanten konfiguriert werden, darunter die folgenden:

- **Datenspeicherort** Der primäre Geschäftssitz der Organisation, an dem die Daten aufbewahrt werden sollen.
- **Datenaufbewahrung** Der Standardaufbewahrungszeitraum beträgt sechs Monate, kann aber geändert werden.
- **Vorschaufunktionen** Die Vorschaufunktionen sind standardmäßig aktiviert.

Das Microsoft Endpoint Manager Admin Center bietet ein All-in-One-Administrationszentrum für die Geräteanmeldung, Geräte- und Konfigurationskonformität, Endpunktsicherheit und für weitere Berichtsfunktionen. Die integrierten Berichte sind in vier Schwerpunktbereiche eingeteilt.

- **Operative Berichte** Gezielte und handlungsorientierte Daten
- **Organisationsberichte** Zusammenfassende Übersichten auf hoher Ebene für eine Organisation
- **Trendberichte** Zeigt Muster und Trends über einen bestimmten Zeitraum an.
- **Erweiterte Berichte** Ermöglicht es Ihnen, die zugrunde liegenden Daten zu verwenden, um Ihre eigenen benutzerdefinierten Berichte zu erstellen.

Abbildung 1–1 zeigt die Standard-Startseite des Microsoft Endpoint Manager Admin Center mit Berichten zum Status gesunder und aktiver Geräte.

> ***HINWEIS***
>
> **Um die Protokolle, die als Teil der Berichte verwendet werden, zu überprüfen, müssen Sie entweder die Rolle des globalen Administrators oder des Intune-Dienstadministrators oder die Rolle des Intune-Administrators mit Leserechten besitzen.**

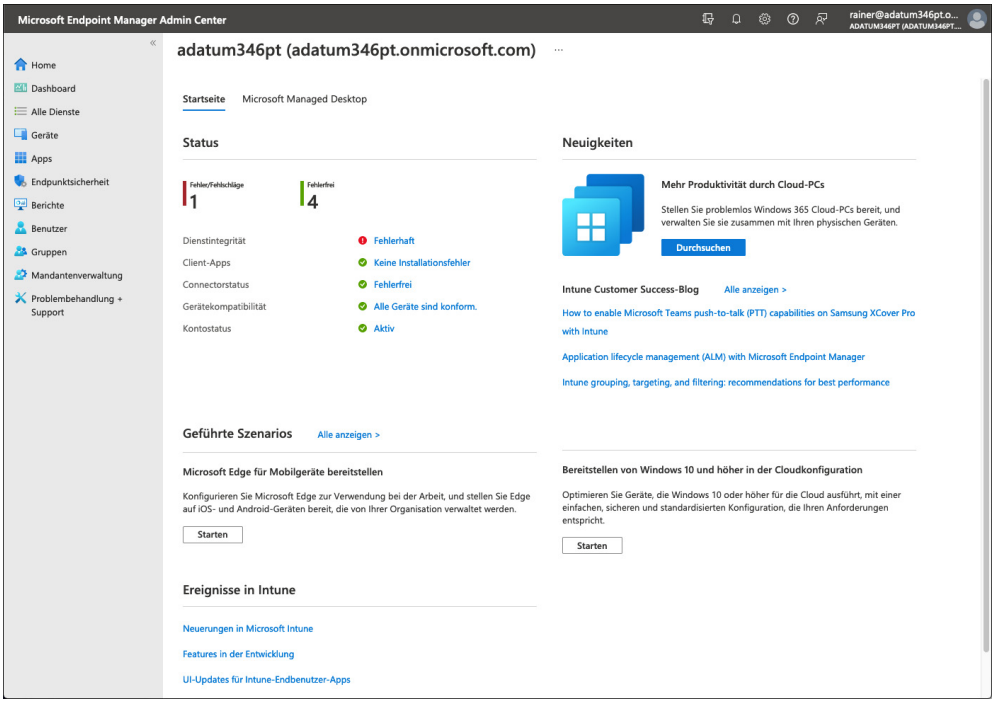

Abb. 1–1 Microsoft Endpoint Manager Admin Center

Microsoft Endpoint Manager-Implementierung planen

Microsoft bietet eine Kombination von Endpunktlösungen an, die über das Microsoft Endpoint Manager Admin Center verwaltet werden. Diese Angebote haben sich im Laufe der Jahre verändert, wobei stark in Clouddienste und die Integration mit Azure investiert wurde. Die Einführung von Windows 10 hat auch die Art und Weise beeinflusst, wie Sie Geräte mit einer Reihe von nativen MDM-Protokollen (Mobile Device Management) innerhalb des Betriebssystems verwalten, wodurch die Notwendigkeit entfällt, auf Ihren Endpunkten einen weiteren Agenten zu installieren. Welche Lösung Sie wählen sollten, hängt von den Bereitstellungszielen Ihres Unternehmens ab. Die beiden wichtigsten Geräteverwaltungslösungen von Microsoft sind:

- **Microsoft Intune** Diese Lösung eignet sich am besten für Kunden, die moderne Verwaltungsfunktionen für Windows 10-Geräte benötigen, aber gleichzeitig auch ihre lokale Serverinfrastruktur einschränken müssen. Microsoft Intune ist eine cloudbasierte Verwaltungslösung, die keine zusätzliche Serverinfrastruktur erfordert. Die Plattformunterstützung für Intune umfasst Verwaltungsfunktionen für Windows 10 und macOS. Sie haben außerdem Zugriff auf Funktionen wie Autopilot, die dazu beitragen können, die Anforderungen für die Bereitstellung herkömmlicher Betriebssysteme zu reduzieren.
- **Co-Management zwischen Microsoft Intune und ConfigMgr** Diese Lösung stellt eine Brücke zwischen Microsoft Intune und ConfigMgr dar und ermöglicht Kunden die gemeinsame Verwaltung von Geräten auf der Grundlage ihrer Anforderungen. ConfigMgr ist eine Vor-Ort-Verwaltungslösung mit zusätzlicher Plattformunterstützung, z.B. für Windows Server. Sie umfasst auch eine Reihe einzigartiger Technologien, wie z.B. Tasksequenzen und Image-Bereitstellung. Umgebungen mit Co-Management können Workloads für ihre Windows 10-Geräte und mobilen Geräte in die Cloud verlagern und gleichzeitig die traditionelle Infrastruktur unterstützen.

Intune einrichten

Zur Einrichtung von Intune sind mehrere Schritte erforderlich, bevor Sie Geräte verwalten können. Diese Schritte sind wie folgt:

1. **Verstehen der unterstützten Konfigurationen** Dazu gehören das unterstützte Gerätebetriebssystem, die Netzwerkanforderungen und die Unterschiede zwischen der kommerziellen und der speziell auf Behörden ausgerichteten Cloud.
2. **Erstellen Sie ein Abonnement** Fügen Sie Intune zu Ihrem Mandanten hinzu und berücksichtigen Sie dabei, ob Sie ein Microsoft Online Services-Konto, ein Enterprise Agreement oder einen Volumenlizenzvertrag haben.
3. **Konfigurieren Sie einen benutzerdefinierten Domänennamen** Konfigurieren Sie einen benutzerdefinierten Domänennamen oder einen Vanity-Domänennamen zur Verwendung mit Ihrem Mandanten. Es wird empfohlen, dies vor dem Hinzufügen von Benutzerkonten zu tun, um die Kontoverwaltung zu vereinfachen.

4. **Benutzer und Gruppen hinzufügen** Fügen Sie einzelne Benutzer und Gruppen zu Intune hinzu. Alternativ können Sie eine Verbindung zu Active Directory mit Intune für die Synchronisierung herstellen.
5. **Lizenzen zuweisen** Verknüpfen Sie erworbene Intune- oder Enterprise Mobility + Security-Lizenzen mit Benutzerkonten.
6. **Legen Sie die MDM-Autorität fest** Dies gilt nur für Mandanten mit einem Service-Release vor 1911. Mandanten, die 1911 oder später verwenden, werden automatisch für Intune konfiguriert.
7. **Apps zuweisen** Apps können Gruppen zur automatischen oder optionalen Installation zugewiesen werden.
8. **Geräte konfigurieren** Konfigurieren Sie die Profile, die die Geräteeinstellungen und Gerätefeatures verwalten.
9. **Anpassen der Portale** Fügen Sie den verschiedenen Portalen Ihr Firmenbranding hinzu.
10. **Aktivieren Sie die Geräteregistrierung** Aktivieren Sie bestimmte Geräte, die für die Verwaltung durch Intune registriert werden sollen.
11. **Anwendungsrichtlinien konfigurieren** Konfigurieren Sie spezifische Anwendungsschutzrichtlinien für von Intune geschützte Anwendungen.

PRÜFUNGSTIPP

Bei einigen Prüfungsaufgaben müssen Sie die Reihenfolge der Schritte zur Konfiguration einer Lösung verstehen. So müssen beispielsweise Lizenzen und die MDM-Autorität konfiguriert werden, bevor Sie die Geräteregistrierung konfigurieren können.

WEITERE INFORMATIONEN **Microsoft Intune einrichten**

Eine ausführliche Schritt-für-Schritt-Anleitung für die Einrichtung von Intune finden Sie unter *https://docs.microsoft.com/de-de/mem/intune/fundamentals/setup-steps*.

Lizenzen zuweisen

Sie können Benutzern Intune-Lizenzen sowohl über das Microsoft Endpoint Manager Admin Center als auch über das Azure-Portal in Azure Active Directory zuweisen. Gehen Sie folgendermaßen vor, um eine Lizenz über das Admin Center zuzuweisen:

1. Melden Sie sich beim Microsoft Endpoint Manager Admin Center unter *https://endpoint.microsoft.com* an.
2. Klicken Sie auf **Benutzer**.
3. Klicken Sie auf **Alle Benutzer** und dann auf den Benutzer, für den Sie die Lizenzzuweisungen ändern möchten.
4. Klicken Sie auf **Lizenzen** und dann auf **Zuweisungen**.