

Powercamp: Microsoft 365 Certified – Enterprise Administrator Expert

Zertifizierung zum Microsoft 365 Admin-Profi

Wissensgarantie: 12 Monate

Trainings-ID: [PCM365Enterprise](#)

Hersteller-ID: [MS-102](#)

Hersteller-ID: [MS-102](#)

Examen: [MS-102](#)

Examen: [MS-102](#)

[Zum Seminar →](#)

Das nehmen Sie mit

Microsoft 365 ist die cloudbasierte Produktivitätsplattform von Microsoft für Endkunden und Businesskunden. Mit einem Abonnement für Microsoft 365 erhalten Sie die neuesten Produktivitäts-Apps wie Microsoft Teams, OneDrive, Sharepoint Online, Exchange Online und Microsoft 365 for Business/Enterprise und vieles mehr.

Microsoft 365 umfasst ebenso zusätzliche Sicherheits- und Compliance-Funktionen sowie Windows-Lizenzen zusätzlich zu den Kerndiensten.

Dieses Powercamp mit erweiterten Kurszeiten geht ganz speziell auf die Einrichtung, Konfiguration und Verwaltung eines Microsoft 365-Tenants einschließlich Verwaltung von Identitäten, Sicherheitskonfigurationen und Umsetzung von Compliance Anforderungen von Microsoft 365 ein.

Des Weiteren sind die Vorbereitungen für die Examen MS-102 und SC-300 ein Schwerpunkt dieses Powercamps. Bei erfolgreichem Abschluss beider Examen erreichen Sie den Titel „Microsoft 365 certified: Administrator Expert“.

Folgende IT-Jobroles werden in diesem Training behandelt:

Microsoft 365-Administrator*innen

Microsoft 365-Administrator*innen fungieren als Integrationshub für alle Microsoft 365-Workloads. Sie koordinieren mehrere Microsoft 365-Workloads. Zudem arbeiten sie mit Lösungsarchitekt*innen und anderen Administrator*innen zusammen, die für Workloads, Infrastrukturen, Identitäten, Sicherheit, Compliance, Endpunkte und Anwendungen verantwortlich sind.

Microsoft-Identitäts- und Zugriffs-Administrator*innen

Der Microsoft-Identitäts- und Zugriffs-Administrator entwirft, implementiert und betreibt die Systeme zur Identitäts- und Zugriffsverwaltung einer Organisation mithilfe von Microsoft Azure Active Directory (Azure AD), das Bestandteil von Microsoft Entra ist. Sie konfigurieren und verwalten die Authentifizierung und Autorisierung von Identitäten für Benutzer*innen, Geräte, Azure-Ressourcen und -Anwendungen.

Die Identitäts- und Zugriffsadministrator*innen stellen nahtlose Benutzerumgebungen und Self-Service-Verwaltungsfunktionen für alle Benutzer*innen bereit. Sie stellen sicher, dass die Identität explizit überprüft wird, um Zero Trust-Prinzipien umzusetzen. Sie automatisieren die Verwaltung von Azure AD mithilfe von PowerShell und analysieren Ereignisse mit der Kusto-Abfragesprache (KQL). Außerdem sind sie für die Problembehandlung, das Überwachen und die Berichterstellung für die Identitäts- und Zugriffsumgebung verantwortlich.

Identitäts- und Zugriffsadministrator*innen arbeiten mit vielen anderen Rollen in der Organisation zusammen, um strategische Identitätsprojekte zum Modernisieren von Identitätslösungen zu fördern sowie Hybrididentitätslösungen und Identitätsgovernance zu implementieren.

Sie sollten mit Azure- und Microsoft 365-Diensten und -Workloads vertraut sein.

Nach Besuch dieses Trainings haben die Teilnehmer*innen Kenntnisse zu folgenden Themen:

- Bereitstellen und Verwalten eines Microsoft 365-Mandanten
- Verwalten von Benutzern und Gruppen
- Implementieren und Verwalten externer Identitäten

- Implementieren und Verwalten einer Hybrididentität
- Planen, Implementieren und Verwalten der Azure Multi-Factor Authentication (MFA) und Self-Service-Kennwortzurücksetzung
- Planen, Implementieren und Verwalten der Azure AD-Benutzerauthentifizierung
- Planen, Implementieren und Verwalten des bedingten Zugriffs für Azure AD
- Verwalten von Azure AD Identity Protection
- Implementieren der Zugriffsverwaltung für Azure-Ressourcen
- Verwalten und Überwachen des Anwendungszugriffs mithilfe von Microsoft Defender for Cloud Apps
- Planen, Implementieren und Überwachen der Integration von Unternehmensanwendungen
- Planen und Implementieren von Anwendungsregistrierungen
- Planen und Implementieren der Berechtigungsverwaltung
- Planen, Implementieren und Verwalten von Zugriffsüberprüfungen
- Planen und Implementieren von privilegiertem Zugriff
- Überwachen von Azure AD
- Verwalten von Sicherheitsberichten und Warnungen mithilfe des Microsoft 365 Defender-Portals
- Implementieren und Verwalten des E-Mail- und Zusammenarbeitsschutzes mithilfe von Microsoft Defender for Office 365
- Implementieren und Verwalten von Endpoint Protection mithilfe von Microsoft Defender for Endpoint
- Implementieren von Microsoft Purview Information Protection und der Datenlebenszyklusverwaltung
- Implementieren von Microsoft Purview Data Loss Prevention (DLP)

Das nehmen Sie mit

Microsoft 365 ist die cloudbasierte Produktivitätsplattform von Microsoft für Endkunden und Businesskunden. Mit einem Abonnement für Microsoft 365 erhalten Sie die neuesten Produktivitäts-Apps wie Microsoft Teams, OneDrive, Sharepoint Online, Exchange Online und Microsoft 365 for Business/Enterprise und vieles mehr.

Microsoft 365 umfasst ebenso zusätzliche Sicherheits- und Compliance-Funktionen sowie Windows-Lizenzen zusätzlich zu den Kerndiensten.

Dieses Powercamp mit erweiterten Kurszeiten geht ganz speziell auf die Einrichtung, Konfiguration und Verwaltung eines Microsoft 365-Tenants einschließlich Verwaltung von Identitäten, Sicherheitskonfigurationen und Umsetzung von Compliance Anforderungen von Microsoft 365 ein.

Des Weiteren sind die Vorbereitungen für die Examen MS-102 und SC-300 ein Schwerpunkt dieses Powercamps. Bei erfolgreichem Abschluss beider Examen erreichen Sie den Titel „Microsoft 365 certified: Administrator Expert“.

Folgende IT-Jobroles werden in diesem Training behandelt:

Microsoft 365-Administrator*innen

Microsoft 365-Administrator*innen fungieren als Integrationshub für alle Microsoft 365-Workloads. Sie koordinieren mehrere Microsoft 365-Workloads. Zudem arbeiten sie mit Lösungsarchitekt*innen und anderen Administrator*innen zusammen, die für Workloads, Infrastrukturen, Identitäten, Sicherheit, Compliance, Endpunkte und Anwendungen verantwortlich sind.

Microsoft-Identitäts- und Zugriffs-Administrator*innen

Der Microsoft-Identitäts- und Zugriffs-Administrator entwirft, implementiert und betreibt die Systeme zur Identitäts- und Zugriffsverwaltung einer Organisation mithilfe von Microsoft Azure Active Directory (Azure AD), das Bestandteil von Microsoft Entra ist. Sie konfigurieren und verwalten die Authentifizierung und Autorisierung von Identitäten für Benutzer*innen, Geräte, Azure-Ressourcen und -Anwendungen.

Die Identitäts- und Zugriffsadministrator*innen stellen nahtlose Benutzerumgebungen und Self-Service-Verwaltungsfunktionen für alle Benutzer*innen bereit. Sie stellen sicher, dass die Identität explizit überprüft wird, um Zero Trust-Prinzipien umzusetzen. Sie automatisieren die Verwaltung von Azure AD mithilfe von PowerShell und analysieren Ereignisse mit der Kusto-Abfragesprache (KQL). Außerdem sind sie für die Problembehandlung, das Überwachen und die

Berichterstellung für die Identitäts- und Zugriffsumgebung verantwortlich.

Identitäts- und Zugriffsadministrator*innen arbeiten mit vielen anderen Rollen in der Organisation zusammen, um strategische Identitätsprojekte zum Modernisieren von Identitätslösungen zu fördern sowie Hybrididentitätslösungen und Identitätsgovernance zu implementieren.

Sie sollten mit Azure- und Microsoft 365-Diensten und -Workloads vertraut sein.

Nach Besuch dieses Trainings haben die Teilnehmer*innen Kenntnisse zu folgenden Themen:

- Bereitstellen und Verwalten eines Microsoft 365-Mandanten
- Verwalten von Benutzern und Gruppen
- Implementieren und Verwalten externer Identitäten
- Implementieren und Verwalten einer Hybrididentität
- Planen, Implementieren und Verwalten der Azure Multi-Factor Authentication (MFA) und Self-Service-Kennwortzurücksetzung
- Planen, Implementieren und Verwalten der Azure AD-Benutzerauthentifizierung
- Planen, Implementieren und Verwalten des bedingten Zugriffs für Azure AD
- Verwalten von Azure AD Identity Protection
- Implementieren der Zugriffsverwaltung für Azure-Ressourcen
- Verwalten und Überwachen des Anwendungszugriffs mithilfe von Microsoft Defender for Cloud Apps
- Planen, Implementieren und Überwachen der Integration von Unternehmensanwendungen
- Planen und Implementieren von Anwendungsregistrierungen
- Planen und Implementieren der Berechtigungsverwaltung
- Planen, Implementieren und Verwalten von Zugriffsüberprüfungen
- Planen und Implementieren von privilegiertem Zugriff
- Überwachen von Azure AD
- Verwalten von Sicherheitsberichten und Warnungen mithilfe des Microsoft 365 Defender-Portals
- Implementieren und Verwalten des E-Mail- und Zusammenarbeitsschutzes mithilfe von Microsoft Defender for Office 365

- Implementieren und Verwalten von Endpoint Protection mithilfe von Microsoft Defender for Endpoint
- Implementieren von Microsoft Purview Information Protection und der Datenlebenszyklusverwaltung
- Implementieren von Microsoft Purview Data Loss Prevention (DLP)

Zielgruppen

- Administrator*innen für Microsoft 365
- Prüfungsanwärter*innen

Wichtige Informationen

Dieses Training wird seit Dezember 2023 nicht mehr in dieser Form angeboten.

Unser neues Powercamp zum Thema Microsoft 365 – Enterprise Administrator:

PCM365EE Powercamp: Microsoft 365 Certified – Enterprise Administrator Expert

Termine & Optionen