

Einführung

1 Minute

100 XP

In diesem Modul erhalten Sie eine Einführung in einige der Features und Tools, die Sie verwenden können, um die Governance Ihrer Azure-Umgebung zu optimieren. Darüber hinaus erfahren Sie mehr über Tools, die Sie verwenden können, um Ressourcen in Übereinstimmung mit Unternehmensanforderungen oder gesetzlichen Anforderungen zu halten.

Lernziele

Nach Abschluss dieses Moduls können Sie folgende Aufgaben durchführen:

- Beschreiben des Zwecks von Microsoft Purview
- Beschreiben des Zwecks von Azure Policy
- Beschreiben des Zwecks von Ressourcensperren
- Beschreiben des Zwecks des Service Trust Portal

Nächste Lektion: Beschreiben des Zwecks von Microsoft Purview

Beschreiben des Zwecks von Microsoft Purview

100 XP

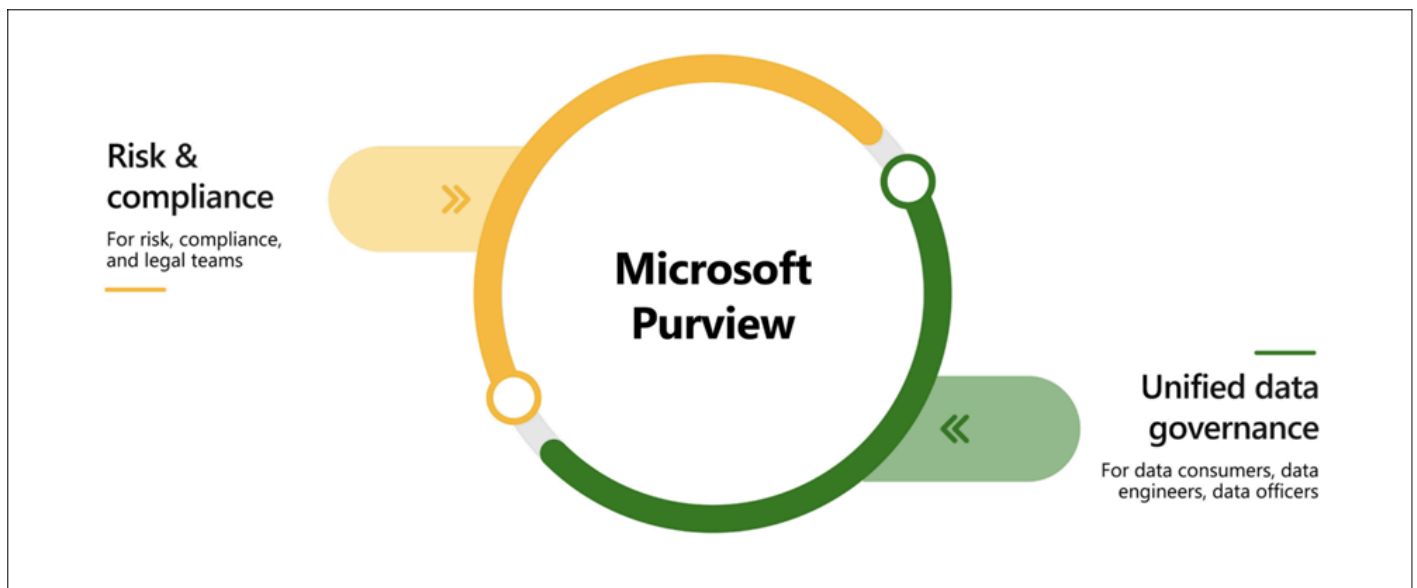
3 Minuten

Bei Microsoft Purview handelt es sich um eine Familie von Datengovernance-, Risiko- und Compliancelösungen, mit denen Sie einen zentralen, einheitlichen Überblick über Ihre Daten erhalten können. Microsoft Purview bietet Erkenntnisse über Ihre lokalen Daten, Multi-Cloud- und Software-as-a-Service-Daten.

Mit Microsoft Purview können Sie ihre Datenlandschaft dank folgender Funktionen auf dem neuesten Stand halten:

- Automatisierte Datenermittlung
- Klassifizierung vertraulicher Daten
- Vollständige Datenherkunft

Microsoft Purview umfasst zwei Hauptlösungsbereiche: **Risiko und Compliance** sowie **einheitliche Datengovernance**.



Risiko- und Compliancelösungen in Microsoft Purview

Microsoft 365 ist eine Kernkomponente der Risiko- und Compliancelösungen von Microsoft Purview. Microsoft Teams, OneDrive und Exchange sind nur einige der Microsoft 365-Dienste, mit denen Microsoft Ihre Daten verwaltet und überwacht. Durch die Verwaltung und Überwachung Ihrer Daten kann Microsoft Purview Ihre Organisation wie folgt unterstützen:

- Schützen von vertraulichen Daten in Clouds, Apps und auf Geräten
- Identifizieren von Datenrisiken und Verwalten gesetzlicher Complianceanforderungen
- Erste Schritte mit der Einhaltung gesetzlicher Bestimmungen

Einheitliche Datengovernance

Microsoft Purview bietet robuste, einheitliche Lösungen für Datengovernance, mit der Sie Ihre lokalen, Multi-Cloud- und SaaS-Daten (Software-as-a-Service) verwalten können. Mit den robusten Datengovernancefunktionen von Microsoft Purview können Sie Ihre in Azure-, SQL- und Hive-Datenbanken gespeicherten Daten lokal und sogar in anderen Clouds wie Amazon S3 verwalten.

Die einheitliche Datengovernance von Microsoft Purview ermöglicht Ihrer Organisation Folgendes:

- Erstellen einer aktuellen Übersicht Ihres gesamten Datenbestands, einschließlich Datenklassifizierung und End-to-End-Herkunft
- Ermitteln, wo vertrauliche Daten in Ihrem Datenbestand gespeichert sind
- Erstellen einer sicheren Umgebung für Datenconsumer, um wertvolle Daten zu finden
- Generieren von Erkenntnissen darüber, wie Ihre Daten gespeichert und verwendet werden
- Sicheres Verwalten des Zugriffs auf die Daten in Ihrem Datenbestand im benötigten Umfang

Nächste Lektion: Grundlegendes zum Zweck von Azure Policy

Grundlegendes zum Zweck von Azure Policy

100 XP

3 Minuten

Wie stellen Sie sicher, dass Ihre Ressourcen konform bleiben? Wie können Sie benachrichtigt werden, wenn sich die Konfiguration einer Ressource geändert hat?

Azure Policy ist ein Dienst in Azure, der es Ihnen ermöglicht, Richtlinien zu erstellen, zuzuweisen und zu verwalten, die Ihre Ressourcen steuern oder überwachen. Mit diesen Richtlinien werden unterschiedliche Regeln für Ressourcenkonfigurationen erzwungen, damit diese Konfigurationen stets mit Ihren Unternehmensstandards konform bleiben.

Wie definiert Azure Policy Richtlinien?

Mit Azure Policy können Sie sowohl einzelne Richtlinien als auch Gruppen verwandter Richtlinien definieren, die als Initiativen bezeichnet werden. Azure Policy wertet Ihre Ressourcen aus und hebt die Ressourcen hervor, die nicht mit den von Ihnen erstellten Richtlinien konform sind. Azure Policy kann auch verhindern, dass nicht konforme Ressourcen erstellt werden.

Azure-Richtlinien können auf jeder Ebene festgelegt werden, sodass Sie Richtlinien für eine bestimmte Ressource, eine Ressourcengruppe, ein Abonnement usw. festlegen können. Azure-Richtlinien werden außerdem vererbt. Wenn Sie also eine Richtlinie auf einer höheren Ebene festlegen, wird sie automatisch auf alle Gruppierungen unter der übergeordneten Richtlinie angewendet. Wenn Sie beispielsweise eine Azure-Richtlinie für eine Ressourcengruppe festlegen, wird diese Richtlinie von allen in dieser Ressourcengruppe erstellten Ressourcen automatisch übernommen.

Azure Policy enthält integrierte Richtlinien- und Initiativendefinitionen für Speicher, Netzwerk, Compute, Security Center und Überwachung. Wenn Sie beispielsweise eine Richtlinie definieren, die nur eine bestimmte Größe für die virtuellen Computer (VMs) in Ihrer Umgebung zulässt, wird diese Richtlinie beim Erstellen einer neuen VM und bei jeder Größenänderung vorhandener VMs aufgerufen. Darüber hinaus werden mit Azure Policy auch alle aktuellen VMs in der Umgebung ausgewertet und überwacht, darunter auch VMs, die vor der Richtlinie erstellt wurden.

In einigen Fällen kann Azure Policy nicht konforme Ressourcen und Konfigurationen automatisch korrigieren, um die Integrität des Zustands der Ressourcen zu gewährleisten. Wenn zum Beispiel alle Ressourcen in einer bestimmten Ressourcengruppe mit dem Tag „AppName“ und dem Wert „SpecialOrders“ gekennzeichnet werden sollen, wendet Azure Policy dieses Tag automatisch erneut an, wenn es fehlt. Sie behalten jedoch weiterhin die vollständige Kontrolle über Ihre Umgebung. Wenn Sie über eine bestimmte Ressource verfügen, die von Azure Policy nicht automatisch korrigiert werden soll, können Sie diese Ressource als Ausnahme kennzeichnen, sodass diese Ressource durch die Richtlinie nicht automatisch korrigiert wird.

Azure Policy kann auch in Azure DevOps integriert werden, indem alle Continuous Integration- bzw. Continuous Delivery-Pipelinerichtlinien angewendet werden, die sich auf die Schritte vor und nach der Bereitstellung Ihrer Anwendungen beziehen.

Was sind Azure Policy-Initiativen?

Eine Azure Policy-Initiative ist eine Möglichkeit, verwandte Richtlinien zu gruppieren. Eine Initiativendefinition enthält alle Richtliniendefinitionen, um Ihren Konformitätsstatus zur Erreichung eines größeren Ziels besser nachverfolgen können.

Azure Policy enthält z. B. eine Initiative namens Überwachung in Azure Security Center aktivieren. Ihr Ziel ist es, alle verfügbaren Sicherheitsempfehlungen für alle Azure-Ressourcentypen in Azure Security Center zu überwachen.

Im Rahmen dieser Initiative sind die folgenden Richtliniendefinitionen enthalten:

- **Überwachung von unverschlüsselten SQL-Datenbanken in Security Center:** Diese Richtlinie dient zum Überwachen von unverschlüsselten SQL-Datenbanken und -Servern.
- **Überwachung von Betriebssystem-Sicherheitsrisiken in Security Center:** Diese Richtlinie überwacht Server, welche die konfigurierte Sicherheitsrisikobaseline des Betriebssystems nicht erfüllen.
- **Überwachung des fehlenden Endpoint Protection-Schutzes in Security Center:** Diese Richtlinie überwacht Server, auf denen kein Endpoint Protection-Agent installiert ist.

Tatsächlich enthält die Initiative Überwachung in Azure Security Center aktivieren mehr als 100 separate Richtliniendefinitionen.

Nächste Lektion: Beschreiben des Zwecks von Ressourcensperren

Beschreiben des Zwecks von Ressourcensperren

100 XP

3 Minuten

Eine Ressourcensperre verhindert, dass Ressourcen versehentlich gelöscht oder geändert werden.

Auch wenn Azure RBAC-Richtlinien (rollenbasierte Azure-Zugriffssteuerung) vorhanden sind, besteht immer noch das Risiko, dass Personen mit der richtigen Zugriffsebene wichtige Cloudressourcen löschen könnten. Ressourcensperren verhindern abhängig vom Sperrtyp, dass Ressourcen gelöscht oder aktualisiert werden. Ressourcensperren können auf einzelne Ressourcen, Ressourcengruppen oder sogar ein gesamtes Abonnement angewendet werden. Ressourcensperren werden vererbt, d. h. wenn Sie eine Ressourcensperre auf eine Ressourcengruppe anwenden, gilt diese auch für alle Ressourcen in der Ressourcengruppe.

Typen von Ressourcensperren

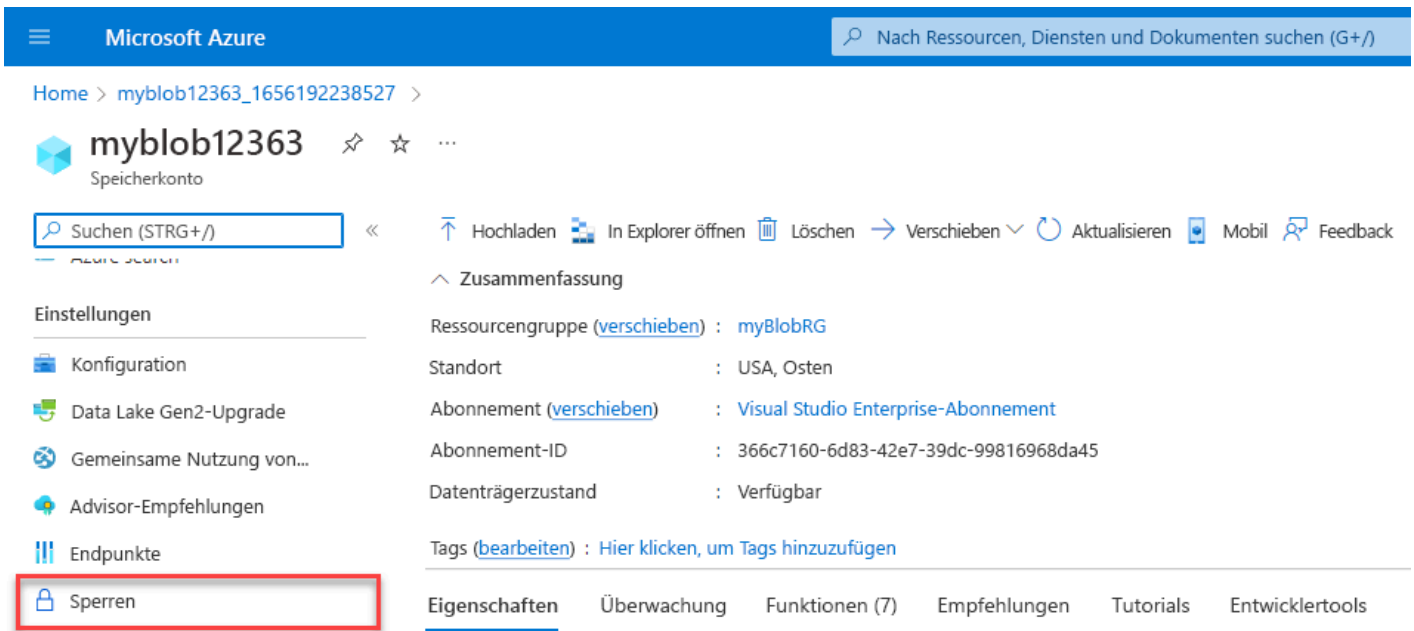
Es gibt zwei Arten von Ressourcensperren: eine, die verhindert, dass Benutzer*innen Ressourcen löschen, und eine, die verhindert, dass Benutzer*innen eine Ressource ändern oder löschen.

- Löschen bedeutet, dass autorisierte Benutzer*innen eine Ressource weiterhin lesen und ändern, jedoch nicht löschen können.
- ReadOnly bedeutet, dass autorisierte Benutzer eine Ressource zwar lesen, aber nicht löschen oder aktualisieren können. Mit dieser Sperre erzielen Sie einen ähnlichen Effekt wie durch die Beschränkung sämtlicher autorisierter Benutzer auf die Berechtigungen der Leserolle.

Wie verwalte ich Ressourcensperren?

Sie können Ressourcensperren über das Azure-Portal, mit PowerShell, der Azure-CLI oder über eine Azure Resource Manager-Vorlage verwalten.

Um Sperren im Azure-Portal anzuzeigen, hinzuzufügen oder zu löschen, navigieren Sie im Azure-Portal im Bereich Einstellungen einer beliebigen Ressource zum Abschnitt Einstellungen.



The screenshot shows the Microsoft Azure portal interface for a storage account named 'myblob12363'. The left sidebar contains navigation options, with 'Sperren' (Locks) highlighted by a red rectangle. The main content area shows the account's summary, including its resource group, location, subscription, and tags. The 'Eigenschaften' (Properties) tab is selected.

Wie lösche oder ändere ich eine gesperrte Ressource?

Obwohl das Sperren dabei hilft, versehentliche Änderungen zu verhindern, können Sie weiterhin Änderungen vornehmen, indem Sie einen zweistufigen Vorgang ausführen.

Um eine gesperrte Ressource zu ändern, müssen Sie zunächst die Sperre entfernen. Nachdem Sie die Sperre entfernt haben, können Sie jede beliebige Aktion anwenden, die Sie ausführen dürfen. Ressourcensperren gelten unabhängig von RBAC-Berechtigungen. Selbst wenn Sie Besitzer der Ressource sind, müssen Sie die Sperre aufheben, ehe Sie die blockierte Aktivität tatsächlich durchführen können.

Nächste Lektion: Übung: Konfigurieren einer Ressourcensperre

Übung: Konfigurieren einer Ressourcensperre

100 XP

15 Minuten

In dieser Übung erstellen Sie eine Ressource und konfigurieren eine Ressourcensperre. Speicherkonten stellen eine der einfachsten Möglichkeiten für Ressourcensperren dar, die Auswirkungen schnell zu ermitteln, weshalb Sie für diese Übung ein Speicherkonto verwenden.

Dies ist eine Bring-Your-Own-Subscription-Übung, was bedeutet, dass Sie Ihr eigenes Azure-Abonnement bereitstellen müssen, um die Übung abschließen zu können. Aber keine Sorge: Wenn Sie sich für ein Azure-Konto registrieren, können Sie die gesamte Übung ohne Zusatzkosten mit den für zwölf Monate kostenlosen Diensten abschließen.

Falls Sie Hilfe bei der Registrierung eines Azure-Kontos benötigen, finden Sie Informationen im Lernmodul Erstellen eines Azure-Kontos.

Führen Sie die folgenden Schritte aus, nachdem Sie Ihr kostenloses Konto erstellt haben. Wenn Sie nicht über ein Azure-Konto verfügen, können Sie die Schritte durchgehen, um mehr über den Prozess zum Hinzufügen einer einfachen Ressourcensperre für eine Ressource zu erfahren.

Aufgabe 1: Erstellen einer Ressource

Um eine Ressourcensperre anzuwenden, müssen Sie über eine Ressource verfügen, die in Azure erstellt wurde. Der Fokus der ersten Aufgabe liegt auf der Erstellung einer Ressource, die Sie dann in nachfolgenden Aufgaben sperren können.

1. Melden Sie sich unter <https://portal.azure.com> beim Azure-Portal an.
2. Wählen Sie Ressource erstellen.
3. Wählen Sie unter Kategorien die Option Speicher aus.
4. Wählen Sie unter „Speicherkonto“ die Option „Neu erstellen“ aus.
5. Geben Sie auf der Registerkarte „Grundlagen“ des Blatts „Speicherkonto erstellen“ die folgenden Informationen ein. Belassen Sie ansonsten die Standardeinstellungen.

Tabelle erweitern

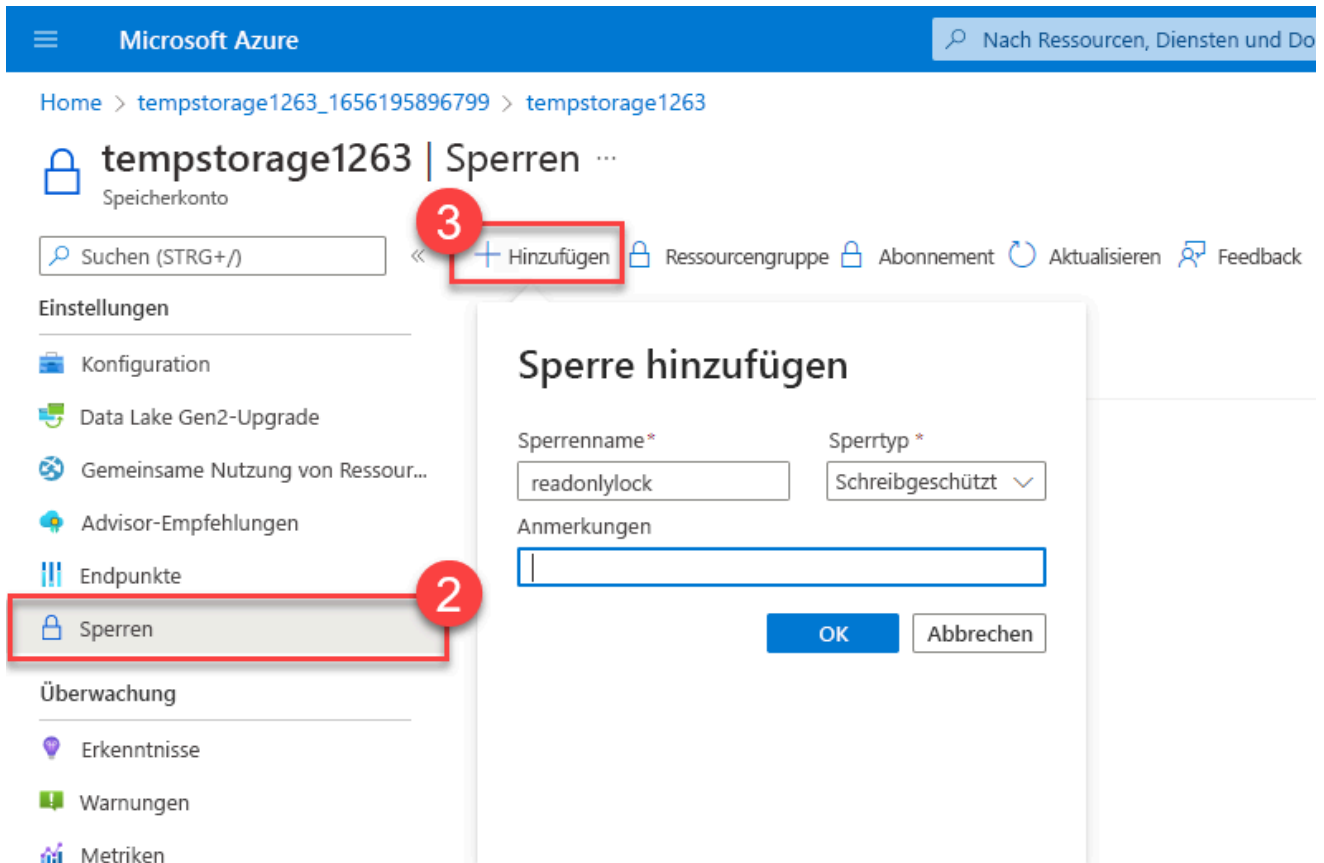
Einstellung	Wert
Resource group	Neu erstellen
Speicherkontoname	Geben Sie einen eindeutigen Speicherkontonamen ein.
Standort	default
Leistung	Standard
Redundanz	Lokal redundanter Speicher (LRS)

6. Klicken Sie auf „Überprüfen + erstellen“, um die Einstellungen Ihres Speicherkontos zu überprüfen und Azure die Validierung der Konfiguration zu ermöglichen.
7. Klicken Sie nach der Validierung auf „Erstellen“. Warten Sie auf die Benachrichtigung, dass das Konto erfolgreich erstellt wurde.
8. Auswählen von „Zu Ressource wechseln“

Aufgabe 2: Anwenden einer Schreibschutzsperre für Ressourcen

In dieser Aufgabe wenden Sie eine Schreibschutzsperre für Ressourcen auf das Speicherkonto an. Was denken Sie, welche Auswirkungen dies auf das Speicherkonto hat?

1. Scrollen Sie nach unten, bis der Abschnitt „Einstellungen“ des Blatts auf der linken Seite des Bildschirms angezeigt wird.
2. Wählen Sie Sperren aus.
3. Wählen Sie + Hinzufügen.



4. Geben Sie einen Namen für die Sperre ein.
5. Überprüfen Sie, ob der Sperrtyp auf „Schreibgeschützt“ festgelegt ist.
6. Wählen Sie „OK“ aus.

Aufgabe 3: Hinzufügen eines Containers zum Speicherkonto

In dieser Aufgabe fügen Sie einen Container zum Speicherkonto hinzu. In diesem Container können Sie Ihre Blobs speichern.

1. Scrollen Sie nach oben, bis der Abschnitt „Datenspeicher“ des Blatts auf der linken Seite des Bildschirms angezeigt wird.
2. Wählen Sie Container aus.
3. Wählen Sie + Container aus.

Microsoft Azure

Home > tempstorage1263_1656195896799 > tempstorage1263

tempstorage1263 | Container

Speicherkonto

Suchen (STRG+ /)

+ Container

Zugriffsebene... Container wieder... Aktualisieren Löschen

Container nach Präfix durchsuchen

Name

☐ \$logs

Übersicht

Aktivitätsprotokoll

Tags

Diagnose und Problembeh...

Zugriffssteuerung (IAM)

Datenmigration

Ereignisse

Speicherbrowser (Vorschau)

Datenspeicher

Container

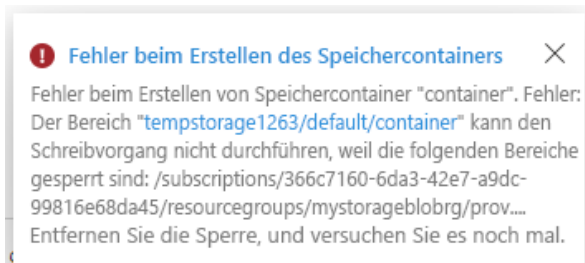
Dateifreigaben

Warteschlangen

Tabellen

4. Geben Sie einen Containernamen ein, und klicken Sie auf „Erstellen“.

5. Die Fehlermeldung „Fehler beim Erstellen des Speichercontainers“ sollte angezeigt werden.



Hinweis

Die Fehlermeldung informiert Sie darüber, dass Sie aufgrund einer eingerichteten Sperre keinen Speichercontainer erstellen können. Die Schreibschutzsperre verhindert alle Erstellungs- oder Aktualisierungsvorgänge im Speicherkonto, sodass Sie keinen Speichercontainer erstellen können.

Aufgabe 4: Ändern der Ressourcensperre und Erstellen eines Speichercontainers

1. Scrollen Sie nach unten, bis der Abschnitt „Einstellungen“ des Blatts auf der linken Seite des Bildschirms angezeigt wird.
2. Wählen Sie Sperren aus.
3. Wählen Sie die Schreibschutzsperre für Ressourcen aus, die Sie erstellt haben.
4. Ändern Sie den Sperrtyp in „Löschen“, und klicken Sie auf „OK“.

Microsoft Azure

Home > tempstorage1263_1656195896799 > tempstorage1263

tempstorage1263 | Sperren ...
Storage account

Suchen (STRG+ /) << + Hinzufügen 🔒 Ressource... 🔒 Abonnement ↻ Aktualisieren 🗨 Feedback

Shared Access Signature

Verschlüsselung

Microsoft Defender for Cloud

Datenverwaltung

- Geo-replication
- Data protection
- Object replication
- Blob inventory
- Statische Website
- Lebenszyklusverwaltung
- Azure Search

Einstellungen

- Konfiguration
- Data Lake Gen2-Upgrade
- Gemeinsame Nutzung von Res...
- Advisor recommendations
- Endpunkte
- Sperren**

Sperrenname	Lock type	Bereich
storagelock	Schreibgeschützt	tempstorage1263

Sperre bearbeiten

storagelock

Lock type *

Schreibgeschützt

Schreibgeschützt

Löschen

Löschen OK Abbrechen

5. Scrollen Sie nach oben, bis der Abschnitt „Datenspeicher“ des Blatts auf der linken Seite des Bildschirms angezeigt wird.

6. Wählen Sie Container aus.

7. Wählen Sie + Container aus.

8. Geben Sie einen Containernamen ein, und klicken Sie auf „Erstellen“.

9. Ihr Speichercontainer sollte in der Liste der Container angezeigt werden.

Sie verstehen nun, wie die Schreibschutzsperre verhindert hat, dass Sie Ihrem Speicherkonto einen Container hinzufügen. Nachdem der Sperrtyp geändert wurde (hätte stattdessen ggf. entfernt werden können), konnten Sie einen Container hinzufügen.

Aufgabe 5: Löschen des Speicherkontos

Diese letzte Aufgabe müssen Sie zweimal ausführen. Denken Sie daran, dass es eine Löchsperre für das Speicherkonto gibt, sodass Sie das Speicherkonto noch nicht löschen können.

1. Scrollen Sie nach oben, bis oben auf dem Blatt auf der linken Seite des Bildschirms „Übersicht“ angezeigt wird.
2. Wählen Sie „Übersicht“ aus.
3. Wählen Sie „Löschen“ aus.

Microsoft Azure

Home >

tempstorage1263 Speicherkonto

Suchen (STRG+ /)

Übersicht

Aktivitätsprotokoll

Tags

Diagnose und Problembehandlung

Zugriffssteuerung (IAM)

Datenmigration

Ereignisse

Speicherbrowser (Vorschau)

Hochladen In Explorer...

Löschen

Verschieben

Aktualisieren

Mobil

Feedback

Zusammenfassung

Resource group (verschieben): mystorageblobrg

Standort: USA, Osten

Subscription (verschieben): Visual Studio Enterprise-Abonnement

Abonnement-ID: 366c7160-6da3-42e7-a9dc-99816e68da45

Datenträgerzustand: Verfügbar

Tags (bearbeiten): Hier klicken, um Tags hinzuzufügen

Eigenschaften Überwachung Funktionen (7) Empfehlungen Tutorials Entwicklertools

Sie sollten eine Benachrichtigung erhalten, die Sie darüber informiert, dass Sie die Ressource aufgrund einer Löschsperre nicht löschen können. Um das Speicherkonto löschen zu können, müssen Sie die Löschsperre entfernen.

Microsoft Azure

Home > tempstorage1263 >

Speicherkonto löschen


tempstorage1263

"tempstorage1263" kann nicht gelöscht werden, weil diese Ressource oder ihr übergeordnetes Element eine Löschsperre aufweist. Die Sperren müssen entfernt werden, damit diese Ressource gelöscht werden kann. [Weitere Informationen zu Löschsperren](#)

Aufgabe 6: Entfernen der Löschsperre und Löschen des Speicherkontos

In der letzten Aufgabe entfernen Sie die Ressourcensperre und löschen das Speicherkonto aus Ihrem Azure-Konto. Dieser Schritt ist wichtig. Sie möchten sicherstellen, dass Sie in Ihrem Konto nicht über eine Leerlaufressource verfügen.

1. Wählen Sie ihren Speicherkontonamen auf der Breadcrumb-Leiste oben auf dem Bildschirm aus.
2. Scrollen Sie nach unten, bis der Abschnitt „Einstellungen“ des Blatts auf der linken Seite des Bildschirms angezeigt wird.
3. Wählen Sie Sperren aus.
4. Wählen Sie „Löschen“ aus.
5. Klicken Sie auf der Breadcrumb-Leiste oben auf dem Bildschirm auf „Startseite“.
6. Auswählen von Speicherkonten
7. Wählen Sie das für diese Übung verwendete Speicherkonto aus.
8. Wählen Sie „Löschen“ aus.
9. Um das versehentliche Löschen zu verhindern, fordert Azure Sie auf, den Namen des zu löschenden Speicherkontos einzugeben. Geben Sie den Namen des Speicherkontos ein, und klicken Sie auf „Löschen“.





 Microsoft Azure Nach Ressourcen, Dienst


Home > tempstorage1263 >

Speicherkonto löschen ...

tempstorage1263

Die folgende Tabelle zeigt die Liste der Speicherdienste. Sie können auf die Liste klicken, um auf Daten darin zuzugreifen.

	Blobs
	Dateien
	Tabellen
	Warteschlangen

 Diese Aktion kann nicht rückgängig gemacht werden. Hierdurch wird das Speicherkonto „tempstorage1263“ und dessen Inhalt dauerhaft gelöscht. Wenn eine unveränderliche Richtlinie auf das Konto oder auf beliebige Container oder Blobs angewendet wird, wird das Konto nicht gelöscht.

Geben Sie den Namen des Speicherkontos (tempstorage1263) zur Bestätigung ein:

tempstorage1263 ✓

Löschen

10. Es sollte eine Nachricht angezeigt werden, dass das Speicherkonto gelöscht wurde. Wenn Sie zu „Startseite“ > „Speicherkonten“ navigieren, sollten Sie bemerken, dass das für diese Übung erstellte Speicherkonto nicht mehr vorhanden ist.

Glückwunsch! Sie haben die Übung abgeschlossen, indem Sie eine Ressourcensperre für eine Azure-Ressource konfiguriert, aktualisiert und wieder entfernt haben.

Wichtig

Stellen Sie sicher, dass Sie Aufgabe 6 (Löschen des Speicherkontos) abschließen. Sie sind ausschließlich für die Ressourcen in Ihrem Azure-Konto verantwortlich. Bereinigen Sie Ihr Konto nach Abschluss dieser Übung.

Nächste Lektion: Beschreiben des Zwecks von Service Trust Portal

Beschreiben des Zwecks von Service Trust Portal

100 XP

3 Minuten

Über Microsoft Service Trust Portal erhalten Sie Zugriff auf eine Vielfalt an Inhalten, Tools und weiteren Ressourcen zu den Themen Sicherheit, Datenschutz und Compliance bei Microsoft.

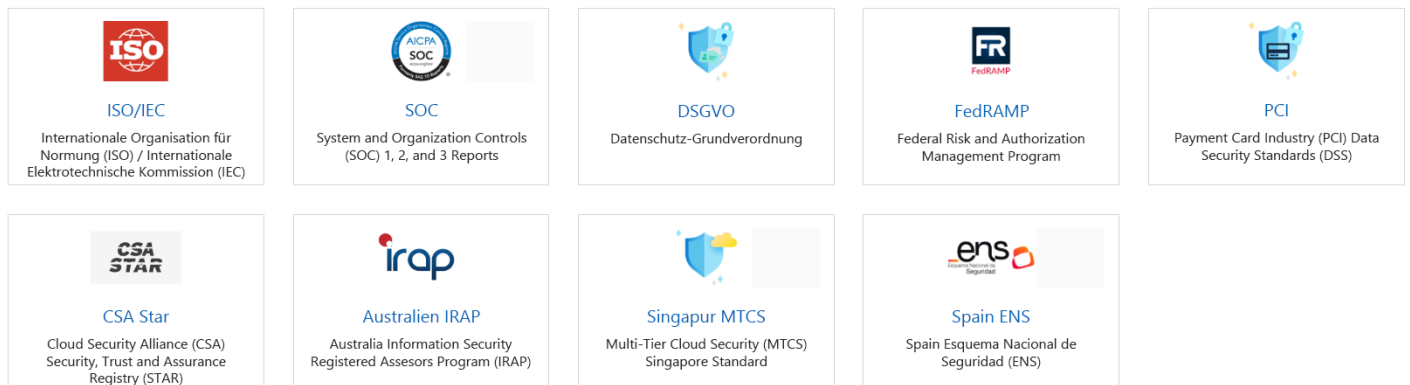
Das Service Trust Portal enthält Details zur Implementierung von Steuerungen und Prozessen von Microsoft, die unsere Clouddienste und die darin enthaltenen Kundendaten schützen. Für den Zugriff auf einige Ressourcen in Service Trust Portal müssen Sie sich als authentifizierter Benutzer/authentifizierte Benutzerin mit Ihrem Microsoft Cloud Services-Konto (Microsoft Entra-Unternehmenskonto) anmelden. Lesen und akzeptieren Sie die Geheimhaltungsvereinbarung von Microsoft für Compliancematerialien.

Zugreifen auf Service Trust Portal

Unter <https://servicetrust.microsoft.com/> können Sie auf Service Trust Portal zugreifen.



Zertifizierungen, Vorschriften und Standards



Auf die Features und Inhalte von Service Trust Portal können Sie über das Hauptmenü zugreifen. Das Hauptmenü enthält folgende Kategorien:

- Über **Service Trust Portal** können Sie schnell zur Startseite von Service Trust Portal zurückkehren.
- Unter **Meine Bibliothek** können Sie Ihre Dokumente speichern (oder anheften), um auf der Seite „Meine Bibliothek“ schnell darauf zugreifen zu können. Sie können auch einrichten, dass Sie bei der Aktualisierung von Dokumenten in „Meine Bibliothek“ benachrichtigt werden.
- **Alle Dokumente** ist eine zentrale Zielseite für Dokumente im Service Trust Portal. Unter **Alle Dokumente** können Sie Dokumente anheften, damit sie unter **Meine Bibliothek** angezeigt werden.

Hinweis

Service Trust Portal-Berichte und -Dokumente können mindestens 12 Monate nach der Veröffentlichung oder bis zur Verfügbarkeit einer neuen Dokumentversion heruntergeladen werden.

Nächste Lektion: Wissensbeurteilung

[Vorherige](#)