



Azure-Berechtigungen und erforderliche Sicherheitsregeln

NetApp Console setup and administration

NetApp
February 11, 2026

Inhalt

- Azure-Berechtigungen und erforderliche Sicherheitsregeln. 1
 - Azure-Berechtigungen für den Konsolen-Agent. 1
 - So werden Azure-Berechtigungen verwendet 4
 - Änderungsprotokoll 20
 - Sicherheitsgruppenregeln für Konsolen-Agents in Azure. 22
 - Eingehende Regeln 23
 - Ausgangsregeln 23

Azure-Berechtigungen und erforderliche Sicherheitsregeln

Azure-Berechtigungen für den Konsolen-Agent

Wenn die NetApp Console einen Konsolenagenten in Azure startet, weist sie der VM eine benutzerdefinierte Rolle zu, die dem Agenten die Berechtigung zum Verwalten von Ressourcen und Prozessen innerhalb dieses Azure-Abonnements erteilt. Der Agent verwendet die Berechtigungen, um API-Aufrufe an mehrere Azure-Dienste zu tätigen.

Ob Sie diese benutzerdefinierte Rolle für den Agenten erstellen müssen, hängt davon ab, wie Sie sie bereitgestellt haben.

Bereitstellen über die NetApp Console

Wenn Sie die Konsole verwenden, um die Agent-VM in Azure bereitzustellen, ermöglicht dies eine ["systemseitig zugewiesene verwaltete Identität"](#) auf der virtuellen Maschine, erstellt eine benutzerdefinierte Rolle und weist sie der virtuellen Maschine zu. Die Rolle stellt der Konsole die erforderlichen Berechtigungen zum Verwalten von Ressourcen und Prozessen innerhalb dieses Azure-Abonnements zur Verfügung. Die Berechtigungen der Rolle werden beim Upgrade des Agenten auf dem neuesten Stand gehalten. Sie müssen diese Rolle für den Agenten nicht erstellen oder Updates verwalten.

Manuelle Bereitstellung oder Bereitstellung über den Azure Marketplace

Wenn Sie den Agenten vom Azure Marketplace bereitstellen oder den Agenten manuell auf einem Linux-Host installieren, müssen Sie die benutzerdefinierte Rolle selbst einrichten und ihre Berechtigungen bei allen Änderungen beibehalten.

Sie müssen sicherstellen, dass die Rolle auf dem neuesten Stand ist, da in nachfolgenden Versionen neue Berechtigungen hinzugefügt werden. Wenn neue Berechtigungen erforderlich sind, werden diese in den Versionshinweisen aufgeführt.

- Schritt-für-Schritt-Anleitungen zur Verwendung dieser Richtlinien finden Sie auf den folgenden Seiten:
 - ["Einrichten von Berechtigungen für eine Azure Marketplace-Bereitstellung"](#)
 - ["Einrichten von Berechtigungen für lokale Bereitstellungen"](#)
 - ["Berechtigungen für den eingeschränkten Modus einrichten"](#)

```
{
  "Name": "Console Operator",
  "Actions": [
    "Microsoft.Compute/disks/delete",
    "Microsoft.Compute/disks/read",
    "Microsoft.Compute/disks/write",
    "Microsoft.Compute/locations/operations/read",
    "Microsoft.Compute/locations/vmSizes/read",
    "Microsoft.Resources/subscriptions/locations/read",
    "Microsoft.Compute/operations/read",
    "Microsoft.Compute/virtualMachines/instanceView/read",
    "Microsoft.Compute/virtualMachines/powerOff/action",
```

```
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/virtualMachines/restart/action",
"Microsoft.Compute/virtualMachines/deallocate/action",
"Microsoft.Compute/virtualMachines/start/action",
"Microsoft.Compute/virtualMachines/vmSizes/read",
"Microsoft.Compute/virtualMachines/write",
"Microsoft.Compute/images/read",
"Microsoft.Network/locations/operationResults/read",
"Microsoft.Network/locations/operations/read",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Network/networkInterfaces/write",
"Microsoft.Network/networkInterfaces/join/action",
"Microsoft.Network/networkSecurityGroups/read",
"Microsoft.Network/networkSecurityGroups/write",
"Microsoft.Network/networkSecurityGroups/join/action",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Network/virtualNetworks/subnets/write",
"Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",
"Microsoft.Network/virtualNetworks/virtualMachines/read",
"Microsoft.Network/virtualNetworks/subnets/join/action",
"Microsoft.Resources/deployments/operations/read",
"Microsoft.Resources/deployments/read",
"Microsoft.Resources/deployments/write",
"Microsoft.Resources/resources/read",
"Microsoft.Resources/subscriptions/operationresults/read",
"Microsoft.Resources/subscriptions/resourceGroups/delete",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/subscriptions/resourcegroups/resources/read",
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Storage/checknameavailability/read",
"Microsoft.Storage/operations/read",
"Microsoft.Storage/storageAccounts/listkeys/action",
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/delete",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Storage/storageAccounts/blobServices/containers/read",
"Microsoft.Storage/storageAccounts/listAccountSas/action",
"Microsoft.Storage/usages/read",
"Microsoft.Compute/snapshots/write",
"Microsoft.Compute/snapshots/read",
"Microsoft.Compute/availabilitySets/write",
"Microsoft.Compute/availabilitySets/read",
"Microsoft.Compute/disks/beginGetAccess/action",
```

```
"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/read",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/write",
    "Microsoft.Network/loadBalancers/read",
    "Microsoft.Network/loadBalancers/write",
    "Microsoft.Network/loadBalancers/delete",
    "Microsoft.Network/loadBalancers/backendAddressPools/read",
    "Microsoft.Network/loadBalancers/backendAddressPools/join/action",
    "Microsoft.Network/loadBalancers/loadBalancingRules/read",
    "Microsoft.Network/loadBalancers/probes/read",
    "Microsoft.Network/loadBalancers/probes/join/action",
    "Microsoft.Authorization/locks/*",
    "Microsoft.Network/routeTables/join/action",
    "Microsoft.NetApp/netAppAccounts/read",
    "Microsoft.NetApp/netAppAccounts/capacityPools/read",
    "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/write",
    "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/read",
    "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete",
    "Microsoft.Network/privateEndpoints/write",

"Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/action",
    "Microsoft.Storage/storageAccounts/privateEndpointConnections/read",
    "Microsoft.Storage/storageAccounts/managementPolicies/read",
    "Microsoft.Storage/storageAccounts/managementPolicies/write",
    "Microsoft.Network/privateEndpoints/read",
    "Microsoft.Network/privateDnsZones/write",
    "Microsoft.Network/privateDnsZones/virtualNetworkLinks/write",
    "Microsoft.Network/virtualNetworks/join/action",
    "Microsoft.Network/privateDnsZones/A/write",
    "Microsoft.Network/privateDnsZones/read",
    "Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",
    "Microsoft.Resources/deployments/operationStatuses/read",
    "Microsoft.Insights/Metrics/Read",
    "Microsoft.Compute/virtualMachines/extensions/write",
    "Microsoft.Compute/virtualMachines/extensions/delete",
    "Microsoft.Compute/virtualMachines/extensions/read",
    "Microsoft.Compute/virtualMachines/delete",
    "Microsoft.Network/networkInterfaces/delete",
    "Microsoft.Network/networkSecurityGroups/delete",
    "Microsoft.Resources/deployments/delete",
    "Microsoft.Compute/diskEncryptionSets/read",
    "Microsoft.Compute/snapshots/delete",
    "Microsoft.Network/privateEndpoints/delete",
```

```

"Microsoft.Compute/availabilitySets/delete",
"Microsoft.KeyVault/vaults/read",
"Microsoft.KeyVault/vaults/accessPolicies/write",
"Microsoft.Compute/diskEncryptionSets/write",
"Microsoft.KeyVault/vaults/deploy/action",
"Microsoft.Compute/diskEncryptionSets/delete",
"Microsoft.Resources/tags/read",
"Microsoft.Resources/tags/write",
"Microsoft.Resources/tags/delete",
"Microsoft.Network/applicationSecurityGroups/write",
"Microsoft.Network/applicationSecurityGroups/read",

"Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/action",
"Microsoft.Network/networkSecurityGroups/securityRules/write",
"Microsoft.Network/applicationSecurityGroups/delete",
"Microsoft.Network/networkSecurityGroups/securityRules/delete",
"Microsoft.Synapse/workspaces/write",
"Microsoft.Synapse/workspaces/read",
"Microsoft.Synapse/workspaces/delete",
"Microsoft.Synapse/register/action",
"Microsoft.Synapse/checkNameAvailability/action",
"Microsoft.Synapse/workspaces/operationStatuses/read",
"Microsoft.Synapse/workspaces/firewallRules/read",
"Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/action",
"Microsoft.Synapse/workspaces/operationResults/read",

"Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/action",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
"Microsoft.Compute/images/write",
"Microsoft.Network/loadBalancers/frontendIPConfigurations/read",
"Microsoft.Compute/virtualMachineScaleSets/write",
"Microsoft.Compute/virtualMachineScaleSets/read",
"Microsoft.Compute/virtualMachineScaleSets/delete"
],
"NotActions": [],
"AssignableScopes": [],
"Description": "Console Permissions",
"IsCustom": "true"
}

```

So werden Azure-Berechtigungen verwendet

In den folgenden Abschnitten wird beschrieben, wie die Berechtigungen für jedes NetApp -Speichersystem und jeden Datendienst verwendet werden. Diese Informationen können hilfreich sein, wenn Ihre Unternehmensrichtlinien vorschreiben, dass Berechtigungen nur bei Bedarf erteilt werden.

Azure NetApp Files

Der Agent stellt die folgenden API-Anforderungen, wenn Sie die NetApp Data Classification zum Scannen von Azure NetApp Files -Daten verwenden:

- NetApp/netAppAccounts/read
- NetApp/netAppAccounts/capacityPools/read
- Microsoft. NetApp/netAppAccounts/capacityPools/volumes/write
- Microsoft. NetApp/netAppAccounts/capacityPools/volumes/read
- Microsoft. NetApp/netAppAccounts/capacityPools/volumes/delete

NetApp Backup and Recovery

In den folgenden Abschnitten wird beschrieben, wie Berechtigungen für NetApp Backup and Recovery verwendet werden.

Minimale NetApp Backup and Recovery

Der Console-Agent stellt die folgenden API-Anfragen für die grundlegende NetApp Backup and Recovery :

- Microsoft.Storage/storageAccounts/listkeys/action
- Microsoft.Storage/storageAccounts/read
- Microsoft.Storage/storageAccounts/write
- Microsoft.Storage/storageAccounts/blobServices/containers/read
- Microsoft.Storage/storageAccounts/listAccountSas/action
- Microsoft.Resources/subscriptions/locations/read
- Microsoft.Resources/subscriptions/resourceGroups/read
- Microsoft.Resources/subscriptions/resourcegroups/resources/read
- Microsoft.Resources/subscriptions/resourceGroups/write
- Microsoft.Storage/storageAccounts/managementPolicies/read
- Microsoft.Storage/storageAccounts/managementPolicies/write
- Microsoft.Authorization/locks/write
- Microsoft.Authorization/locks/read

Nachfolgend finden Sie eine benutzerdefinierte Richtlinie für Sicherung und Wiederherstellung, die mit möglichst wenigen Berechtigungen und einem möglichst engen Geltungsbereich arbeitet:

```

{
  "id":
"/subscriptions/{subscriptionId}/providers/Microsoft.Authorization/roleDef
initions/{roleDefinitionGuid}",
  "properties": {
    "roleName": "Custom Role",
    "description": "Minimal permissions required for Backup and
Recovery.",
    "assignableScopes": [
      "/subscriptions/{subscriptionId}",

"/subscriptions/{subscriptionId}/resourceGroups/{resourceGroupNameContaini
ngConnectorAndStorageAccount}",

"/subscriptions/{subscriptionId}/resourceGroups/{resourceGroupNameContaini
ngConnectorAndStorageAccount}/providers/Microsoft.Storage/storageAccounts/{
storageAccountNameWithObjectLockPreprovisioned}"
    ],
    "permissions": [
      {
        "actions": [
          "Microsoft.Storage/storageAccounts/listkeys/action",
          "Microsoft.Storage/storageAccounts/read",
          "Microsoft.Storage/storageAccounts/write",

"Microsoft.Storage/storageAccounts/blobServices/containers/read",
          "Microsoft.Storage/storageAccounts/listAccountSas/action",
          "Microsoft.Resources/subscriptions/locations/read",

"Microsoft.Resources/subscriptions/resourcegroups/resources/read",
          "Microsoft.Resources/subscriptions/resourceGroups/write",
          "Microsoft.Resources/subscriptions/resourceGroups/read",
          "Microsoft.Storage/storageAccounts/managementPolicies/read",
          "Microsoft.Storage/storageAccounts/managementPolicies/write",
          "Microsoft.Authorization/locks/write",
          "Microsoft.Authorization/locks/read"
        ],
        "notActions": [],
        "dataActions": [],
        "notDataActions": []
      }
    ]
  }
}

```


Erweiterte Berechtigungen für Datensicherung und -wiederherstellung

Der Konsolenagent stellt die folgenden API-Anfragen für erweiterte Sicherungs- und Wiederherstellungsvorgänge sowie Such- und Wiederherstellungsfunktionen. Diese Berechtigungen ermöglichen die Verwaltung von Netzwerken, Schlüsseltresoren und verwalteten Identitäten:

- Microsoft.KeyVault/vaults/accessPolicies/write
- Microsoft.KeyVault/vaults/read
- Microsoft.ManagedIdentity/userAssignedIdentities/assign/action
- Microsoft.Network/networkInterfaces/delete
- Microsoft.Network/networkInterfaces/read
- Microsoft.Network/networkSecurityGroups/delete
- Microsoft.Network/privateDnsZones/read
- Microsoft.Network/privateDnsZones/write
- Microsoft.Network/privateEndpoints/read
- Microsoft.Network/privateEndpoints/write
- Microsoft.Network/virtualNetworks/join/action
- Microsoft.Resources/deployments/delete

Legacy-Berechtigungen für Sicherung und Wiederherstellung

Der Agent führt die folgenden API-Anfragen aus, wenn Sie die Such- und Wiederherstellungsfunktion verwenden. Diese Berechtigungen benötigen Sie nur, wenn Sie vor der Veröffentlichung von Indexing v2 im Februar 2025 ältere Indexierungsfunktionen aktiviert haben:

- Microsoft.Synapse/workspaces/write
- Microsoft.Synapse/workspaces/read
- Microsoft.Synapse/workspaces/delete
- Microsoft.Synapse/register/action
- Microsoft.Synapse/checkNameAvailability/action
- Microsoft.Synapse/workspaces/operationStatuses/read
- Microsoft.Synapse/workspaces/firewallRules/read
- Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/action
- Microsoft.Synapse/workspaces/operationResults/read
- Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/action

NetApp Data Classification

Der Agent stellt die folgenden API-Anfragen, wenn Sie die Datenklassifizierung verwenden.

Aktion	Für die Einrichtung verwendet?	Wird es für den täglichen Betrieb verwendet?
Microsoft.Compute/Standorte/Operationen/Lesen	Ja	Ja

Aktion	Für die Einrichtung verwendet?	Wird es für den täglichen Betrieb verwendet?
Microsoft.Compute/locations/vmSizes/read	Ja	Ja
Microsoft.Compute/operations/read	Ja	Ja
Microsoft.Compute/virtualMachines/instanceView/read	Ja	Ja
Microsoft.Compute/virtualMachines/powerOff/action	Ja	Nein
Microsoft.Compute/virtualMachines/read	Ja	Ja
Microsoft.Compute/virtualMachines/restart/action	Ja	Nein
Microsoft.Compute/virtualMachines/start/action	Ja	Nein
Microsoft.Compute/virtualMachines/vmSizes/read	Nein	Ja
Microsoft.Compute/virtualMachines/write	Ja	Nein
Microsoft.Compute/images/read	Ja	Ja
Microsoft.Compute/disks/delete	Ja	Nein
Microsoft.Compute/disks/read	Ja	Ja
Microsoft.Compute/disks/write	Ja	Nein
Microsoft.Storage/checknameavailability/read	Ja	Ja
Microsoft.Storage/operations/read	Ja	Ja
Microsoft.Storage/storageAccounts/listkeys/action	Ja	Nein
Microsoft.Storage/storageAccounts/read	Ja	Ja
Microsoft.Storage/storageAccounts/write	Ja	Nein
Microsoft.Storage/storageAccounts/blobServices/containers/read	Ja	Ja
Microsoft.Network/networkInterfaces/read	Ja	Ja
Microsoft.Network/networkInterfaces/write	Ja	Nein
Microsoft.Network/networkInterfaces/join/action	Ja	Nein

Aktion	Für die Einrichtung verwendet?	Wird es für den täglichen Betrieb verwendet?
Microsoft.Network/networkSecurityGroups/read	Ja	Ja
Microsoft.Network/networkSecurityGroups/write	Ja	Nein
Microsoft.Resources/subscriptions/locations/read	Ja	Ja
Microsoft.Network/locations/operationResults/read	Ja	Ja
Microsoft.Network/locations/operations/read	Ja	Ja
Microsoft.Network/virtualNetworks/read	Ja	Ja
Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read	Ja	Ja
Microsoft.Network/virtualNetworks/subnets/read	Ja	Ja
Microsoft.Network/virtualNetworks/subnets/virtualMachines/read	Ja	Ja
Microsoft.Network/virtualNetworks/virtualMachines/read	Ja	Ja
Microsoft.Network/virtualNetworks/subnets/join/action	Ja	Nein
Microsoft.Network/virtualNetworks/subnets/write	Ja	Nein
Microsoft.Network/routeTables/join/action	Ja	Nein
Microsoft.Resources/deployments/operations/read	Ja	Ja
Microsoft.Resources/deployments/read	Ja	Ja
Microsoft.Resources/deployments/write	Ja	Nein
Microsoft.Resources/resources/read	Ja	Ja
Microsoft.Resources/subscriptions/operationresults/read	Ja	Ja
Microsoft.Resources/subscriptions/resourceGroups/delete	Ja	Nein
Microsoft.Resources/subscriptions/resourceGroups/read	Ja	Ja

Aktion	Für die Einrichtung verwendet?	Wird es für den täglichen Betrieb verwendet?
Microsoft.Resources/subscriptions/resourcegroups/resources/read	Ja	Ja
Microsoft.Resources/subscriptions/resourceGroups/write	Ja	Nein

Cloud Volumes ONTAP

Der Agent stellt die folgenden API-Anfragen, um Cloud Volumes ONTAP in Azure bereitzustellen und zu verwalten.

Zweck	Aktion	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Erstellen und Verwalten von VMs	Microsoft.Compute/Standorte/Operationen/Lesen	Ja	Ja	Nein
	Microsoft.Compute/Locations/vmSizes/read	Ja	Ja	Nein
	Microsoft.Resources/subscriptions/locations/read	Ja	Nein	Nein
	Microsoft.Compute/operations/read	Ja	Ja	Nein
	Microsoft.Compute/virtualMachines/instanceView/read	Ja	Ja	Nein
	Microsoft.Compute/virtualMachines/powerOff/action	Ja	Ja	Nein
	Microsoft.Compute/virtualMachines/read	Ja	Ja	Nein
	Microsoft.Compute/virtualMachines/restart/action	Ja	Ja	Nein
	Microsoft.Compute/virtualMachines/start/action	Ja	Ja	Nein
	Microsoft.Compute/virtualMachines/deallocate/action	Nein	Ja	Ja
	Microsoft.Compute/virtualMachines/vmSizes/read	Nein	Ja	Nein
	Microsoft.Compute/virtualMachines/write	Ja	Ja	Nein
	Microsoft.Compute/virtualMachines/delete	Ja	Ja	Ja
	Microsoft.Resources/deployments/delete	Ja	Nein	Nein

Zweck	Aktion	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Aktivieren der Bereitstellung von einer VHD	Microsoft.Compute/images/read	Ja	Nein	Nein
	Microsoft.Compute/images/write	Ja	Nein	Nein
Erstellen und Verwalten von Netzwerkschnittstellen im Zielsubnetz	Microsoft.Network/networkInterfaces/read	Ja	Ja	Nein
	Microsoft.Network/networkInterfaces/write	Ja	Ja	Nein
	Microsoft.Network/networkInterfaces/join/action	Ja	Ja	Nein
	Microsoft.Network/networkInterfaces/delete	Ja	Ja	Nein
Erstellen und Verwalten von Netzwerksicherheitsgruppen	Microsoft.Network/networkSecurityGroups/read	Ja	Ja	Nein
	Microsoft.Network/networkSecurityGroups/write	Ja	Ja	Nein
	Microsoft.Network/networkSecurityGroups/join/action	Ja	Nein	Nein
	Microsoft.Network/networkSecurityGroups/delete	Nein	Ja	Ja

Zweck	Aktion	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Abrufen von Netzwerkinformationen zu Regionen, dem Ziel-VNet und Subnetz und Hinzufügen der VMs zu VNets	Microsoft.Network/locations/operationResults/read	Ja	Ja	Nein
	Microsoft.Network/locations/operations/read	Ja	Ja	Nein
	Microsoft.Network/virtualNetworks/read	Ja	Nein	Nein
	Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read	Ja	Nein	Nein
	Microsoft.Network/virtualNetworks/subnets/read	Ja	Ja	Nein
	Microsoft.Network/virtualNetworks/subnets/virtualMachines/read	Ja	Ja	Nein
	Microsoft.Network/virtualNetworks/virtualMachines/read	Ja	Ja	Nein
	Microsoft.Network/virtualNetworks/subnets/join/action	Ja	Ja	Nein

Zweck	Aktion	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Erstellen und Verwalten von Ressourcengruppen	Microsoft.Resources/deployments/operations/read	Ja	Ja	Nein
	Microsoft.Resources/deployments/read	Ja	Ja	Nein
	Microsoft.Resources/deployments/write	Ja	Ja	Nein
	Microsoft.Resources/resources/read	Ja	Ja	Nein
	Microsoft.Resources/subscriptions/operationresults/read	Ja	Ja	Nein
	Microsoft.Resources/subscriptions/resourceGroups/delete	Ja	Ja	Ja
	Microsoft.Resources/subscriptions/resourceGroups/read	Nein	Ja	Nein
	Microsoft.Resources/subscriptions/resourcegroups/resources/read	Ja	Ja	Nein
	Microsoft.Resources/subscriptions/resourceGroups/write	Ja	Ja	Nein

Zweck	Aktion	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Verwalten von Azure-Speicherkonten und -Datenträgern	Microsoft.Compute/disks/read	Ja	Ja	Ja
	Microsoft.Compute/disks/write	Ja	Ja	Nein
	Microsoft.Compute/disks/delete	Ja	Ja	Ja
	Microsoft.Storage/checknameavailability/read	Ja	Ja	Nein
	Microsoft.Storage/operations/read	Ja	Ja	Nein
	Microsoft.Storage/storageAccounts/listkeys/action	Ja	Ja	Nein
	Microsoft.Storage/storageAccounts/read	Ja	Ja	Nein
	Microsoft.Storage/storageAccounts/delete	Nein	Ja	Ja
	Microsoft.Storage/storageAccounts/write	Ja	Ja	Nein
	Microsoft.Storage/usage/read	Nein	Ja	Nein
Aktivieren Sie Sicherungen im Blob-Speicher und die Verschlüsselung von Speicherkonten	Microsoft.Storage/storageAccounts/blobServices/containers/read	Ja	Ja	Nein
	Microsoft.KeyVault/vaults/read	Ja	Ja	Nein
	Microsoft.KeyVault/vaults/accessPolicies/write	Ja	Ja	Nein
Aktivieren von VNet-Dienstendpunkten für Datentiering	Microsoft.Network/virtualNetworks/subnets/write	Ja	Ja	Nein
	Microsoft.Network/routeTables/join/action	Ja	Ja	Nein

Zweck	Aktion	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Erstellen und Verwalten von Azure-verwalteten Snapshots	Microsoft.Compute/Snapshots/write	Ja	Ja	Nein
	Microsoft.Compute/Snapshots/read	Ja	Ja	Nein
	Microsoft.Compute/Snapshots/delete	Nein	Ja	Ja
	Microsoft.Compute/disks/beginGetAccess/action	Nein	Ja	Nein
Erstellen und Verwalten von Verfügbarkeitsgruppen	Microsoft.Compute/availabilitySets/write	Ja	Nein	Nein
	Microsoft.Compute/availabilitySets/read	Ja	Nein	Nein
Aktivieren Sie programmgesteuerte Bereitstellungen vom Marktplatz aus	Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/read	Ja	Nein	Nein
	Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/write	Ja	Ja	Nein

Zweck	Aktion	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Verwalten eines Load Balancers für HA-Paare	Microsoft.Network/loadBalancers/read	Ja	Ja	Nein
	Microsoft.Network/loadBalancers/write	Ja	Nein	Nein
	Microsoft.Network/loadBalancers/delete	Nein	Ja	Ja
	Microsoft.Network/loadBalancers/backendAddressPools/read	Ja	Nein	Nein
	Microsoft.Network/loadBalancers/backendAddressPools/join/action	Ja	Nein	Nein
	Microsoft.Network/loadBalancers/frontendIPConfigurations/read	Ja	Ja	Nein
	Microsoft.Network/loadBalancers/loadBalancingRules/read	Ja	Nein	Nein
	Microsoft.Network/loadBalancers/probes/read	Ja	Nein	Nein
	Microsoft.Network/loadBalancers/probes/join/action	Ja	Nein	Nein
Aktivieren der Sperrverwaltung auf Azure-Datenträgern	Microsoft.Authorization/locks/*	Ja	Ja	Nein

Zweck	Aktion	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Aktivieren Sie private Endpunkte für HA-Paare, wenn außerhalb des Subnetzes keine Konnektivität besteht.	Microsoft.Network/privateEndpoints/write	Ja	Ja	Nein
	Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/action	Ja	Nein	Nein
	Microsoft.Storage/storageAccounts/privateEndpointConnections/read	Ja	Ja	Ja
	Microsoft.Network/privateEndpoints/read	Ja	Ja	Ja
	Microsoft.Network/privateDnsZones/write	Ja	Ja	Nein
	Microsoft.Network/privateDnsZones/virtualNetworkLinks/write	Ja	Ja	Nein
	Microsoft.Network/virtualNetworks/join/action	Ja	Ja	Nein
	Microsoft.Network/privateDnsZones/A/write	Ja	Ja	Nein
	Microsoft.Network/privateDnsZones/read	Ja	Ja	Nein
	Microsoft.Network/privateDnsZones/virtualNetworkLinks/read	Ja	Ja	Nein
Erforderlich für einige VM-Bereitstellungen, abhängig von der zugrunde liegenden physischen Hardware	Microsoft.Resources/deployments/operationStatuses/read	Ja	Ja	Nein
Entfernen Sie Ressourcen aus einer Ressourcengruppe, falls die Bereitstellung fehlschlägt oder gelöscht wird	Microsoft.Network/privateEndpoints/delete	Ja	Ja	Nein
	Microsoft.Compute/availabilitySets/delete	Ja	Ja	Nein

Zweck	Aktion	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Aktivieren Sie die Verwendung von vom Kunden verwalteten Verschlüsselungsschlüsseln bei der Verwendung der API	Microsoft.Compute/diskEncryptionSets/read	Ja	Ja	Ja
	Microsoft.Compute/diskEncryptionSets/write	Ja	Ja	Nein
	Microsoft.KeyVault/vaults/deploy/action	Ja	Nein	Nein
	Microsoft.Compute/diskEncryptionSets/delete	Ja	Ja	Ja
Konfigurieren Sie eine Anwendungssicherheitsgruppe für ein HA-Paar, um die HA-Verbindung und die Cluster-Netzwerk-NICs zu isolieren.	Microsoft.Network/applicationSecurityGroups/write	Nein	Ja	Nein
	Microsoft.Network/applicationSecurityGroups/read	Nein	Ja	Nein
	Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/action	Nein	Ja	Nein
	Microsoft.Network/networkSecurityGroups/securityRules/write	Ja	Ja	Nein
	Microsoft.Network/applicationSecurityGroups/delete	Nein	Ja	Ja
	Microsoft.Network/networkSecurityGroups/securityRules/delete	Nein	Ja	Ja
Mit Cloud Volumes ONTAP -Ressourcen verknüpfte Tags lesen, schreiben und löschen	Microsoft.Resources/tags/read	Nein	Ja	Nein
	Microsoft.Resources/tags/write	Ja	Ja	Nein
	Microsoft.Resources/tags/delete	Ja	Nein	Nein
Verschlüsseln von Speicherkonten während der Erstellung	Microsoft.ManagedIdentity/userAssignedIdentities/assign/action	Ja	Ja	Nein

Zweck	Aktion	Wird für die Bereitstellung verwendet?	Wird es für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Verwenden Sie Virtual Machine Scale Sets im flexiblen Orchestrierungsmodus, um bestimmte Zonen für Cloud Volumes ONTAP anzugeben	Microsoft.Compute/virtualMachineScaleSets/write	Ja	Nein	Nein
	Microsoft.Compute/virtualMachineScaleSets/read	Ja	Nein	Nein
	Microsoft.Compute/virtualMachineScaleSets/delete	Nein	Nein	Ja

Abstufung

Der Agent stellt die folgenden API-Anfragen, wenn Sie NetApp Cloud Tiering einrichten.

- Microsoft.Storage/storageAccounts/listkeys/action
- Microsoft.Resources/subscriptions/resourceGroups/read
- Microsoft.Resources/subscriptions/locations/read

Der Konsolenagent stellt für den täglichen Betrieb die folgenden API-Anfragen.

- Microsoft.Storage/storageAccounts/blobServices/containers/read
- Microsoft.Storage/storageAccounts/managementPolicies/read
- Microsoft.Storage/storageAccounts/managementPolicies/write
- Microsoft.Storage/storageAccounts/read

Änderungsprotokoll

Wenn Berechtigungen hinzugefügt oder entfernt werden, vermerken wir dies in den folgenden Abschnitten.

11. November 2025

Es wurde eine benutzerdefinierte JSON-Richtlinie hinzugefügt, die die geringstmöglichen Berechtigungen und den kleinstmöglichen Geltungsbereich widerspiegelt.

Folgende Berechtigungen wurden der minimalen Berechtigungsliste für Sicherung und Wiederherstellung hinzugefügt:

- Microsoft.Authorization/locks/write
- Microsoft.Authorization/locks/read

Die folgenden Berechtigungen werden für die Datensicherung und -wiederherstellung nicht mehr benötigt, es sei denn, Sie verwenden die Legacy-Indexierung:

- Microsoft.Synapse/workspaces/write
- Microsoft.Synapse/workspaces/read

- Microsoft.Synapse/workspaces/delete
- Microsoft.Synapse/register/action
- Microsoft.Synapse/checkNameAvailability/action
- Microsoft.Synapse/workspaces/operationStatuses/read
- Microsoft.Synapse/workspaces/firewallRules/read
- Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/action
- Microsoft.Synapse/workspaces/operationResults/read
- Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/action

Die folgenden Berechtigungen wurden in den Abschnitt „Zusätzliche Sicherungs- und Wiederherstellungsberechtigungen“ verschoben, da sie für eine minimale Konfiguration nicht erforderlich sind:

- Microsoft.Storage/storageAccounts/listkeys/action
- Microsoft.Storage/storageAccounts/read
- Microsoft.Storage/storageAccounts/write
- Microsoft.Storage/storageAccounts/blobServices/containers/read
- Microsoft.Storage/storageAccounts/listAccountSas/action
- Microsoft.Resources/subscriptions/locations/read
- Microsoft.Resources/subscriptions/resourceGroups/read
- Microsoft.Resources/subscriptions/resourcegroups/resources/read
- Microsoft.Resources/subscriptions/resourceGroups/write
- Microsoft.Storage/storageAccounts/managementPolicies/read
- Microsoft.Storage/storageAccounts/managementPolicies/write

9. September 2024

Die folgenden Berechtigungen wurden aus der JSON-Richtlinie entfernt, da die Konsole die Erkennung und Verwaltung von Kubernetes-Clustern nicht mehr unterstützt:

- Microsoft.ContainerService/managedClusters/listClusterUserCredential/action
- Microsoft.ContainerService/managedClusters/read

22. August 2024

Die folgenden Berechtigungen wurden der JSON-Richtlinie hinzugefügt, da sie für die Cloud Volumes ONTAP Unterstützung von Virtual Machine Scale Sets erforderlich sind:

- Microsoft.Compute/virtualMachineScaleSets/write
- Microsoft.Compute/virtualMachineScaleSets/read
- Microsoft.Compute/virtualMachineScaleSets/delete

5. Dezember 2023

Die folgenden Berechtigungen werden für NetApp Backup and Recovery beim Sichern von Volumedaten im Azure Blob-Speicher nicht mehr benötigt:

- Microsoft.Compute/virtualMachines/read
- Microsoft.Compute/virtualMachines/start/action
- Microsoft.Compute/virtualMachines/deallocate/action
- Microsoft.Compute/virtualMachines/extensions/delete
- Microsoft.Compute/virtualMachines/delete

Diese Berechtigungen sind für andere Konsolenspeicherdienste erforderlich, sodass sie weiterhin in der benutzerdefinierten Rolle für den Agenten verbleiben, wenn Sie diese anderen Speicherdienste verwenden.

12. Mai 2023

Die folgenden Berechtigungen wurden der JSON-Richtlinie hinzugefügt, da sie für die Verwaltung von Cloud Volumes ONTAP erforderlich sind:

- Microsoft.Compute/images/write
- Microsoft.Network/loadBalancers/frontendIPConfigurations/read

Die folgenden Berechtigungen wurden aus der JSON-Richtlinie entfernt, da sie nicht mehr benötigt werden:

- Microsoft.Storage/storageAccounts/blobServices/containers/write
- Microsoft.Network/publicIPAddresses/delete

23. März 2023

Die Berechtigung „Microsoft.Storage/storageAccounts/delete“ wird für die Datenklassifizierung nicht mehr benötigt.

Diese Berechtigung ist für Cloud Volumes ONTAP weiterhin erforderlich.

5. Januar 2023

Die folgenden Berechtigungen wurden der JSON-Richtlinie hinzugefügt:

- Microsoft.Storage/storageAccounts/listAccountSas/action
- Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/action

Diese Berechtigungen sind für NetApp Backup and Recovery erforderlich.

- Microsoft.Network/loadBalancers/backendAddressPools/join/action

Diese Berechtigung ist für die Bereitstellung von Cloud Volumes ONTAP erforderlich.

Sicherheitsgruppenregeln für Konsolen-Agents in Azure

Die Azure-Sicherheitsgruppe für den Agenten erfordert sowohl eingehende als auch ausgehende Regeln. Die NetApp Console erstellt diese Sicherheitsgruppe automatisch, wenn Sie einen Konsolenagenten von der Konsole aus erstellen. Für andere Installationsoptionen müssen Sie diese Sicherheitsgruppe manuell einrichten.

Eingehende Regeln

Protokoll	Hafen	Zweck
SSH	22	Bietet SSH-Zugriff auf den Agent-Host
HTTP	80	<ul style="list-style-type: none">• Bietet HTTP-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche• Wird während des Upgrade-Prozesses von Cloud Volumes ONTAP verwendet
HTTPS	443	Bietet HTTPS-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche und Verbindungen von der NetApp Data Classification -Instanz
TCP	3128	Bietet Cloud Volumes ONTAP Internetzugang, um AutoSupport Nachrichten an den NetApp Support zu senden. Sie müssen diesen Port nach der Bereitstellung manuell öffnen. "Erfahren Sie, wie der Agent als Proxy für AutoSupport -Nachrichten verwendet wird"

Ausgangsregeln

Die vordefinierte Sicherheitsgruppe für den Agenten öffnet den gesamten ausgehenden Datenverkehr. Wenn das akzeptabel ist, befolgen Sie die grundlegenden Regeln für ausgehende Nachrichten. Wenn Sie strengere Regeln benötigen, verwenden Sie die erweiterten Ausgangsregeln.

Grundlegende Ausgangsregeln

Die vordefinierte Sicherheitsgruppe für den Agenten umfasst die folgenden ausgehenden Regeln.

Protokoll	Hafen	Zweck
Alle TCP	Alle	Der gesamte ausgehende Verkehr
Alle UDP	Alle	Der gesamte ausgehende Verkehr

Erweiterte Ausgangsregeln

Wenn Sie strenge Regeln für den ausgehenden Datenverkehr benötigen, können Sie die folgenden Informationen verwenden, um nur die Ports zu öffnen, die für die ausgehende Kommunikation durch den Agenten erforderlich sind.



Die Quell-IP-Adresse ist der Agent-Host.

Service	Protokoll	Hafen	Ziel	Zweck
API-Aufrufe und AutoSupport	HTTPS	443	Outbound-Internet und ONTAP Cluster-Management-LIF	API-Aufrufe an Azure, an ONTAP, an NetApp Data Classification und Senden von AutoSupport-Nachrichten an NetApp
API-Aufrufe	TCP	8080	Datenklassifizierung	Testen der Datenklassifizierungsinstantz während der Bereitstellung
DNS	UDP	53	DNS	Wird von der Konsole für die DNS-Auflösung verwendet

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.