



Azure 权限和所需安全规则

NetApp Console setup and administration

NetApp
February 11, 2026

目录

- Azure 权限和所需安全规则 1
 - 控制台代理的 Azure 权限 1
 - 如何使用 Azure 权限 4
 - 更改日志 18
 - Azure 中的控制台代理安全组规则 20
 - 进站规则 20
 - 出站规则 21

Azure 权限和所需安全规则

控制台代理的 Azure 权限

当NetApp Console在 Azure 中启动控制台代理时，它会将一个自定义角色附加到 VM，该 VM 为代理提供管理该 Azure 订阅中的资源和流程的权限。代理使用权限对多个 Azure 服务进行 API 调用。

是否需要为代理创建此自定义角色取决于您如何部署它。

从NetApp Console部署

当您使用控制台在 Azure 中部署代理虚拟机时，它会启用 ["系统分配的托管标识"](#)在虚拟机上，创建自定义角色，并将其分配给虚拟机。该角色为控制台提供管理该 Azure 订阅内的资源和流程所需的权限。当代理升级时，角色的权限保持最新。您不需要为代理创建此角色或管理更新。

手动部署或从 Azure 市场部署

当您从 Azure 市场部署代理或在 Linux 主机上手动安装代理时，您需要自行设置自定义角色并在任何更改时维护其权限。

您需要确保角色是最新的，因为后续版本中会添加新的权限。如果需要新的权限，它们将在发行说明中列出。

- 要查看使用这些策略的分步说明，请参阅以下页面：

- ["设置 Azure 市场部署的权限"](#)
- ["设置本地部署的权限"](#)
- ["设置限制模式的权限"](#)

```
{
  "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"
}

```

如何使用 **Azure** 权限

以下部分介绍了如何对每个NetApp存储系统和数据服务使用权限。如果您的公司政策规定仅在需要时提供权限，则此信息会很有帮助。

Azure NetApp Files

当您使用NetApp Data Classification扫描Azure NetApp Files数据时，代理会发出以下 API 请求：

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

- NetApp/netAppAccounts/capacityPools/volumes/read
- NetApp/netAppAccounts/capacityPools/volumes/delete

NetApp Backup and Recovery

以下各节描述了NetApp Backup and Recovery如何使用权限。

NetApp Backup and Recovery权限

控制台代理会发出以下 API 请求以实现基本的NetApp Backup and Recovery功能：

- Microsoft.Storage/storageAccounts/listkeys/action
- Microsoft.Storage/storageAccounts/读取
- Microsoft.Storage/storageAccounts/write
- Microsoft.Storage/storageAccounts/blobServices/containers/read
- Microsoft.Storage/storageAccounts/listAccountSas/action
- Microsoft.Resources/订阅/位置/读取
- Microsoft.Resources/订阅/资源组/读取
- Microsoft.Resources/订阅/资源组/资源/读取
- Microsoft.Resources/订阅/资源组/写入
- Microsoft.Storage/storageAccounts/managementPolicies/读取
- Microsoft.Storage/storageAccounts/managementPolicies/write
- Microsoft.Authorization/locks/write
- Microsoft.Authorization/locks/read

以下是用于备份和恢复的自定义策略，它使用的权限最少，范围也最窄：

```

{
  "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": []
      }
    ]
  }
}

```


高级备份和恢复权限

控制台代理发出以下 API 请求，以实现高级备份和恢复操作以及搜索和恢复功能。这些权限允许管理网络、密钥库和受管身份：

- Microsoft.KeyVault/保管库/访问策略/写入
- Microsoft.KeyVault/保管库/读取
- Microsoft.ManagedIdentity/userAssignedIdentities/分配/操作
- Microsoft.Network/networkInterfaces/删除
- Microsoft.Network/网络接口/读取
- Microsoft.Network/networkSecurityGroups/删除
- Microsoft.Network/privateDnsZones/读取
- Microsoft.Network/privateDnsZones/写入
- Microsoft.Network/privateEndpoints/读取
- Microsoft.Network/privateEndpoints/写入
- Microsoft.Network/virtualNetworks/join/action
- Microsoft.Resources/部署/删除

备份和恢复的旧版权限

当您使用搜索和恢复功能时，代理会发出以下 API 请求。只有在 2025 年 2 月索引版本 v2 发布之前启用了旧版索引功能，才需要这些权限：

- Microsoft.Synapse/工作区/写入
- Microsoft.Synapse/工作区/读取
- Microsoft.Synapse/工作区/删除
- Microsoft.Synapse/注册/操作
- Microsoft.Synapse/checkNameAvailability/操作
- Microsoft.Synapse/工作区/operationStatuses/读取
- Microsoft.Synapse/工作区/防火墙规则/读取
- Microsoft.Synapse/工作区/replaceAllIpFirewallRules/操作
- Microsoft.Synapse/工作区/操作结果/读取
- Microsoft.Synapse/工作区/privateEndpointConnectionsApproval/操作

NetApp Data Classification

当您使用数据分类时，代理会发出以下 API 请求。

操作	用于设置吗？	用于日常运营？
Microsoft.Compute/位置/操作/读取	是	是

操作	用于设置吗?	用于日常运营?
Microsoft.Compute/位置/vmSizes/读取	是	是
Microsoft.Compute/操作/读取	是	是
Microsoft.Compute/virtualMachines/instanceView/读取	是	是
Microsoft.Compute/virtualMachines/powerOff/action	是	否
Microsoft.Compute/虚拟机/读取	是	是
Microsoft.Compute/虚拟机/重启/操作	是	否
Microsoft.Compute/virtualMachines/启动/操作	是	否
Microsoft.Compute/virtualMachines/vmSizes/读取	否	是
Microsoft.Compute/虚拟机/写入	是	否
Microsoft.Compute/图像/读取	是	是
Microsoft.Compute/磁盘/删除	是	否
Microsoft.Compute/磁盘/读取	是	是
Microsoft.Compute/磁盘/写入	是	否
Microsoft.Storage/checknameavailability/读取	是	是
Microsoft.Storage/操作/读取	是	是
Microsoft.Storage/storageAccounts/listkeys/action	是	否
Microsoft.Storage/storageAccounts/读取	是	是
Microsoft.Storage/storageAccounts/write	是	否
Microsoft.Storage/storageAccounts/blobServices/containers/read	是	是
Microsoft.Network/网络接口/读取	是	是
Microsoft.Network/网络接口/写入	是	否
Microsoft.Network/networkInterfaces/join/action	是	否
Microsoft.Network/networkSecurityGroups/读取	是	是
Microsoft.Network/networkSecurityGroups/写入	是	否

操作	用于设置吗?	用于日常运营?
Microsoft.Resources/订阅/位置/读取	是	是
Microsoft.Network/locations/operationResults/read	是	是
Microsoft.Network/位置/操作/读取	是	是
Microsoft.Network/virtualNetworks/读取	是	是
Microsoft.Network/virtualNetworks/checkIpAddressAvailability/读取	是	是
Microsoft.Network/virtualNetworks/子网/读取	是	是
Microsoft.Network/virtualNetworks/子网/virtualMachines/读取	是	是
Microsoft.Network/virtualNetworks/virtualMachines/读取	是	是
Microsoft.Network/virtualNetworks/子网/加入/操作	是	否
Microsoft.Network/virtualNetworks/子网/写入	是	否
Microsoft.Network/routeTables/join/action	是	否
Microsoft.Resources/部署/操作/读取	是	是
Microsoft.Resources/部署/读取	是	是
Microsoft.Resources/部署/写入	是	否
Microsoft.Resources/资源/读取	是	是
Microsoft.Resources/subscriptions/operationresults/read	是	是
Microsoft.Resources/subscriptions/resourceGroups/delete	是	否
Microsoft.Resources/订阅/资源组/读取	是	是
Microsoft.Resources/订阅/资源组/资源/读取	是	是
Microsoft.Resources/订阅/资源组/写入	是	否

Cloud Volumes ONTAP

该代理发出以下 API 请求以在 Azure 中部署和管理 Cloud Volumes ONTAP。

目的	操作	用于部署?	用于日常运营?	用于删除?
创建和管理虚拟机	Microsoft.Compute/ 位置/操作/读取	是	是	否
	Microsoft.Compute/ 位置/vmSizes/读取	是	是	否
	Microsoft.Resources /订阅/位置/读取	是	否	否
	Microsoft.Compute/ 操作/读取	是	是	否
	Microsoft.Compute/v irtualMachines/insta nceView/读取	是	是	否
	Microsoft.Compute/v irtualMachines/powe rOff/action	是	是	否
	Microsoft.Compute/ 虚拟机/读取	是	是	否
	Microsoft.Compute/ 虚拟机/重启/操作	是	是	否
	Microsoft.Compute/v irtualMachines/启动/ 操作	是	是	否
	Microsoft.Compute/v irtualMachines/解除 分配/操作	否	是	是
	Microsoft.Compute/v irtualMachines/vmSi zes/读取	否	是	否
	Microsoft.Compute/ 虚拟机/写入	是	是	否
	Microsoft.Compute/ 虚拟机/删除	是	是	是
	Microsoft.Resources /部署/删除	是	否	否
启用从 VHD 部署	Microsoft.Compute/ 图像/读取	是	否	否
	Microsoft.Compute/ 图像/写入	是	否	否

目的	操作	用于部署?	用于日常运营?	用于删除?
在目标子网中创建和管理网络接口	Microsoft.Network/网络接口/读取	是	是	否
	Microsoft.Network/网络接口/写入	是	是	否
	Microsoft.Network/networkInterfaces/join/action	是	是	否
	Microsoft.Network/networkInterfaces/删除	是	是	否
创建和管理网络安全组	Microsoft.Network/networkSecurityGroups/读取	是	是	否
	Microsoft.Network/networkSecurityGroups/写入	是	是	否
	Microsoft.Network/networkSecurityGroups/加入/操作	是	否	否
	Microsoft.Network/networkSecurityGroups/删除	否	是	是

目的	操作	用于部署?	用于日常运营?	用于删除?
获取有关区域、目标 VNet 和子网的网络信息，并将 VM 添加到 VNet	Microsoft.Network/locations/operationResults/read	是	是	否
	Microsoft.Network/位置/操作/读取	是	是	否
	Microsoft.Network/virtualNetworks/读取	是	否	否
	Microsoft.Network/virtualNetworks/checkIpAddressAvailability/读取	是	否	否
	Microsoft.Network/virtualNetworks/子网/读取	是	是	否
	Microsoft.Network/virtualNetworks/子网/virtualMachines/读取	是	是	否
	Microsoft.Network/virtualNetworks/virtualMachines/读取	是	是	否
	Microsoft.Network/virtualNetworks/子网/加入/操作	是	是	否
创建和管理资源组	Microsoft.Resources/部署/操作/读取	是	是	否
	Microsoft.Resources/部署/读取	是	是	否
	Microsoft.Resources/部署/写入	是	是	否
	Microsoft.Resources/资源/读取	是	是	否
	Microsoft.Resources/subscriptions/operationresults/read	是	是	否
	Microsoft.Resources/subscriptions/resourceGroups/delete	是	是	是
	Microsoft.Resources/订阅/资源组/读取	否	是	否
	Microsoft.Resources/订阅/资源组/资源/读取	是	是	否
	Microsoft.Resources/订阅/资源组/写入	是	是	否

目的	操作	用于部署?	用于日常运营?	用于删除?
管理 Azure 存储帐户和磁盘	Microsoft.Compute/磁盘/读取	是	是	是
	Microsoft.Compute/磁盘/写入	是	是	否
	Microsoft.Compute/磁盘/删除	是	是	是
	Microsoft.Storage/checknameavailability/读取	是	是	否
	Microsoft.Storage/操作/读取	是	是	否
	Microsoft.Storage/storageAccounts/listkeys/action	是	是	否
	Microsoft.Storage/storageAccounts/读取	是	是	否
	Microsoft.Storage/storageAccounts/删除	否	是	是
	Microsoft.Storage/storageAccounts/write	是	是	否
	Microsoft.Storage/使用情况/读取	否	是	否
启用 Blob 存储备份和存储帐户加密	Microsoft.Storage/storageAccounts/blobServices/containers/read	是	是	否
	Microsoft.KeyVault/保管库/读取	是	是	否
	Microsoft.KeyVault/保管库/访问策略/写入	是	是	否
启用 VNet 服务终结点以进行数据分层	Microsoft.Network/virtualNetworks/子网/写入	是	是	否
	Microsoft.Network/routeTables/join/action	是	是	否

目的	操作	用于部署?	用于日常运营?	用于删除?
创建和管理 Azure 托管快照	Microsoft.Compute/快照/写入	是	是	否
	Microsoft.Compute/快照/读取	是	是	否
	Microsoft.Compute/快照/删除	否	是	是
	Microsoft.Compute/磁盘/beginGetAccess/操作	否	是	否
创建和管理可用性集	Microsoft.Compute/可用性集/写入	是	否	否
	Microsoft.Compute/可用性集/读取	是	否	否
启用来自市场的程序化部署	Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/read	是	否	否
	Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/write	是	是	否

目的	操作	用于部署?	用于日常运营?	用于删除?
管理 HA 对的负载均衡器	Microsoft.Network/loadBalancers/读取	是	是	否
	Microsoft.Network/loadBalancers/写入	是	否	否
	Microsoft.Network/loadBalancers/删除	否	是	是
	Microsoft.Network/loadBalancers/backendAddressPools/读取	是	否	否
	Microsoft.Network/loadBalancers/backendAddressPools/join/action	是	否	否
	Microsoft.Network/loadBalancers/frontendIPConfigurations/读取	是	是	否
	Microsoft.Network/loadBalancers/loadBalancingRules/读取	是	否	否
	Microsoft.Network/loadBalancers/探测/读取	是	否	否
	Microsoft.Network/loadBalancers/探测/加入/操作	是	否	否
启用 Azure 磁盘上的锁管理	Microsoft.授权/锁/*	是	是	否

目的	操作	用于部署?	用于日常运营?	用于删除?
当子网外部没有连接时，为 HA 对启用专用端点	Microsoft.Network/privateEndpoints/写入	是	是	否
	Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/action	是	否	否
	Microsoft.Storage/storageAccounts/privateEndpointConnections/读取	是	是	是
	Microsoft.Network/privateEndpoints/读取	是	是	是
	Microsoft.Network/privateDnsZones/写入	是	是	否
	Microsoft.Network/privateDnsZones/virtualNetworkLinks/写入	是	是	否
	Microsoft.Network/virtualNetworks/join/action	是	是	否
	Microsoft.Network/privateDnsZones/A/写入	是	是	否
	Microsoft.Network/privateDnsZones/读取	是	是	否
	Microsoft.Network/privateDnsZones/virtualNetworkLinks/读取	是	是	否
对于某些虚拟机部署是必需的，具体取决于底层物理硬件	Microsoft.Resources/deployments/operationStatuses/read	是	是	否
在部署失败或删除的情况下从资源组中删除资源	Microsoft.Network/privateEndpoints/删除	是	是	否
	Microsoft.Compute/可用性集/删除	是	是	否

目的	操作	用于部署?	用于日常运营?	用于删除?
使用 API 时启用客户管理的加密密钥	Microsoft.Compute/diskEncryptionSets/读取	是	是	是
	Microsoft.Compute/diskEncryptionSets/写入	是	是	否
	Microsoft.KeyVault/保管库/部署/操作	是	否	否
	Microsoft.Compute/diskEncryptionSets/删除	是	是	是
为 HA 对配置应用程序安全组，以隔离 HA 互连和集群网络 NIC	Microsoft.Network/applicationSecurityGroups/写入	否	是	否
	Microsoft.Network/applicationSecurityGroups/读取	否	是	否
	Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/action	否	是	否
	Microsoft.Network/networkSecurityGroups/securityRules/写入	是	是	否
	Microsoft.Network/applicationSecurityGroups/删除	否	是	是
	Microsoft.Network/networkSecurityGroups/securityRules/删除	否	是	是
读取、写入和删除与 Cloud Volumes ONTAP 资源关联的标签	Microsoft.Resources/标签/阅读	否	是	否
	Microsoft.Resources/标签/写入	是	是	否
	Microsoft.Resources/标签/删除	是	否	否
在创建期间加密存储帐户	Microsoft.ManagedIdentity/userAssignedIdentities/分配/操作	是	是	否

目的	操作	用于部署?	用于日常运营?	用于删除?
在灵活编排模式下使用虚拟机规模集来为Cloud Volumes ONTAP指定特定区域	Microsoft.Compute/virtualMachineScaleSets/写入	是	否	否
	Microsoft.Compute/virtualMachineScaleSets/读取	是	否	否
	Microsoft.Compute/virtualMachineScaleSets/删除	否	否	是

分层

当您设置NetApp Cloud Tiering时，代理会发出以下 API 请求。

- Microsoft.Storage/storageAccounts/listkeys/action
- Microsoft.Resources/订阅/资源组/读取
- Microsoft.Resources/订阅/位置/读取

控制台代理针对日常操作发出以下 API 请求。

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

更改日志

当添加和删除权限时，我们会在下面的部分中注明。

2025年11月11日

添加了一个自定义 JSON 策略，该策略体现了尽可能少的权限和尽可能小的范围。

以下权限已添加到最小备份和恢复权限列表中：

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

除非您使用的是旧版索引，否则备份和恢复不再需要以下权限：

- Microsoft.Synapse/工作区/写入
- Microsoft.Synapse/工作区/读取
- Microsoft.Synapse/工作区/删除
- Microsoft.Synapse/注册/操作
- Microsoft.Synapse/checkNameAvailability/操作

- Microsoft.Synapse/工作区/operationStatuses/读取
- Microsoft.Synapse/工作区/防火墙规则/读取
- Microsoft.Synapse/工作区/replaceAllIpFirewallRules/操作
- Microsoft.Synapse/工作区/操作结果/读取
- Microsoft.Synapse/工作区/privateEndpointConnectionsApproval/操作

以下权限已移至“其他备份和恢复权限”部分，因为最小配置不需要这些权限：

- Microsoft.Storage/storageAccounts/listkeys/action
- Microsoft.Storage/storageAccounts/读取
- Microsoft.Storage/storageAccounts/write
- Microsoft.Storage/storageAccounts/blobServices/containers/read
- Microsoft.Storage/storageAccounts/listAccountSas/action
- Microsoft.Resources/订阅/位置/读取
- Microsoft.Resources/订阅/资源组/读取
- Microsoft.Resources/订阅/资源组/资源/读取
- Microsoft.Resources/订阅/资源组/写入
- Microsoft.Storage/storageAccounts/managementPolicies/读取
- Microsoft.Storage/storageAccounts/managementPolicies/write

2024年9月9日

由于控制台不再支持发现和管理 Kubernetes 集群，因此从 JSON 策略中删除了以下权限：

- Microsoft.ContainerService/managedClusters/listClusterUserCredential/操作
- Microsoft.ContainerService/managedClusters/读取

2024年8月22日

以下权限已添加到 JSON 策略中，因为它们是Cloud Volumes ONTAP支持虚拟机规模集所必需的：

- Microsoft.Compute/virtualMachineScaleSets/写入
- Microsoft.Compute/virtualMachineScaleSets/读取
- Microsoft.Compute/virtualMachineScaleSets/删除

2023年12月5日

将卷数据备份到 Azure Blob 存储时，NetApp Backup and Recovery不再需要以下权限：

- Microsoft.Compute/虚拟机/读取
- Microsoft.Compute/virtualMachines/启动/操作
- Microsoft.Compute/virtualMachines/解除分配/操作

- Microsoft.Compute/virtualMachines/扩展/删除
- Microsoft.Compute/虚拟机/删除

其他控制台存储服务需要这些权限，因此如果您使用其他存储服务，它们仍将保留在代理的自定义角色中。

2023年5月12日

以下权限已添加到 JSON 策略，因为它们是Cloud Volumes ONTAP管理所必需的：

- Microsoft.Compute/图像/写入
- Microsoft.Network/loadBalancers/frontendIPConfigurations/读取

以下权限已从 JSON 策略中删除，因为不再需要它们：

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

2023年3月23日

数据分类不再需要“Microsoft.Storage/storageAccounts/delete”权限。

Cloud Volumes ONTAP仍然需要此权限。

2023年1月5日

以下权限已添加到 JSON 策略：

- Microsoft.Storage/storageAccounts/listAccountSas/action
- Microsoft.Synapse/工作区/privateEndpointConnectionsApproval/操作

NetApp Backup and Recovery需要这些权限。

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

Cloud Volumes ONTAP部署需要此权限。

Azure 中的控制台代理安全组规则

代理的 Azure 安全组需要入站和出站规则。当您从控制台创建控制台代理时，NetApp Console会自动创建此安全组。对于其他安装选项，您需要手动设置此安全组。

入站规则

协议	端口	目的
SSH	22	提供对代理主机的 SSH 访问

协议	端口	目的
HTTP	80	- 提供从客户端 Web 浏览器到本地用户界面的 HTTP 访问 - 在Cloud Volumes ONTAP升级过程中使用
HTTPS	443	提供从客户端 Web 浏览器到本地用户界面的 HTTPS 访问，以及来自NetApp Data Classification实例的连接
TCP	3128	为Cloud Volumes ONTAP提供互联网访问权限，以便将AutoSupport消息发送给NetApp支持。部署后您必须手动打开此端口。 "了解如何将代理用作AutoSupport消息的代理"

出站规则

代理的预定义安全组打开所有出站流量。如果可以接受，请遵循基本的出站规则。如果您需要更严格的规则，请使用高级出站规则。

基本出站规则

代理的预定义安全组包括以下出站规则。

协议	端口	目的
所有 TCP	全部	所有出站流量
所有 UDP	全部	所有出站流量

高级出站规则

如果您需要对出站流量制定严格的规则，则可以使用以下信息仅打开代理出站通信所需的端口。



源IP地址是代理主机。

服务	协议	端口	目标	目的
API 调用和AutoSupport	HTTPS	443	出站互联网和ONTAP集群管理 LIF	对 Azure、ONTAP、NetApp Data Classification 的API 调用，以及向NetApp发送AutoSupport消息
API 调用	TCP	8080	数据分类	部署期间探测数据分类实例
DNS	UDP	53	DNS	用于控制台的 DNS 解析

版权信息

版权所有 © 2026 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。