Manage CIFS services

REST API reference

Table of Contents

Manage CIFS services

Manage CIFS services

Overview

A CIFS server is necessary to provide SMB clients with access to the Storage Virtual Machine (SVM). Before you begin, the following prerequisites must be in place:

- At least one SVM LIF must exist on the SVM.
- The LIFs must be able to connect to the DNS servers configured on the SVM and to an Active Directory domain controller of the domain to which you want to join the CIFS server.
- The DNS servers must contain the service location records that are needed to locate the Active Directory domain services.
- The cluster time must be synchronized to within five minutes of the Active Directory domain controller.

Performance monitoring

Performance of the SVM can be monitored by the `metric.*` and `statistics.*` properties. These show the performance of the SVM in terms of IOPS, latency and throughput. The `metric.*` properties denote an average whereas `statistics.*` properties denote a real-time monotonically increasing value aggregated across all nodes.

Information on the CIFS server

You must keep the following in mind when creating the CIFS server:

- The CIFS server name might or might not be the same as the SVM name.
- The CIFS server name can be up to 15 characters in length.
- The following characters are not allowed: @ # * ( ) = + [ ] \| ; : " , < > \ / ?
- You must use the FQDN when specifying the domain.
- The default is to add the CIFS server machine account to the Active Directory "CN=Computer" object.
- You can choose to add the CIFS server to a different organizational unit (OU) by specifying the "organizational_unit" parameter. When specifying the OU, do not specify the domain portion of the distinguished name; only specify the OU or CN portion of the distinguished name. ONTAP appends the value provided for the required "-domain" parameter onto the value provided for the "-ou" parameter to create the Active Directory distinguished name, which is used when joining the Active Directory domain.
- You can optionally choose to add a text comment of up to 256 characters about the CIFS server. If there is a space in the comment text, you must enclose the entire string in quotation marks.
- You can optionally choose to add a comma-delimited list of one or more NetBIOS aliases for the CIFS server.
- The initial administrative status of the CIFS server is "up".
- The <i>large-mtu</i> feature is enabled for the new CIFS server.
- The <i>multichannel</i> feature is disabled for the new CIFS server.
- If LDAP is configured with the *use_start_tls* and *session_security* features, the new CIFS server will also have this property set.

- The security.kdc_encryption and security.advertised_kdc_encryptions fields are mutually exclusive. Use the advertised_kdc_encryptions field to specify the encryption types to be advertised to the Key Distribution Center (KDC) server in the Active Directory domain.

Examples

Creating a CIFS server

To create a CIFS server, use the following API. Note the *return_records=true* query parameter used to obtain the newly created entry in the response.

```
# The API:
POST /api/protocols/cifs/services

# The call:
curl -X POST "https://<mgmt-
ip>/api/protocols/cifs/services?return_timeout=10&return_records=true" -H
"accept: application/json" -H "authorization: Basic <CREDENTIALS>" -H
"Content-Type: application/json" -d "{ \"ad_domain\": { \"fqdn\":
\"ontapavc.com\", \"organizational_unit\": \"CN=Computers\", \"password\":
\"<PASSWORD-FOR-USER>\", \"user\": \"administrator\" }, \"comment\":
\"This CIFS Server Belongs to CS Department\", \"default_unix_user\":
\"string\", \"enabled\": true, \"name\": \"CIFS1\", \"netbios\": {
\"aliases\": [ \"ALIAS_1\", \"ALIAS_2\", \"ALIAS_3\" ], \"enabled\":
false, \"wins_servers\": [ \"10.224.65.20\", \"10.224.65.21\" ] },
\"options\": { \"admin_to_root_mapping\": true, \"advanced_sparse_file\":
true, \"copy_offload\": true, \"fake_open\": true, \"fsctl_trim\": true,
\"junction_reparse\": true, \"large_mtu\": true, \"multichannel\": true,
\"null_user_windows_name\": \"string\", \"path_component_cache\": true,
\"referral\": false, \"smb_credits\": 128, \"widelink_reparse_versions\":
[ \"smb1\" ] }, \"security\": { \"encrypt_dc_connection\": false,
\"kdc_encryption\": false, \"restrict_anonymous\": \"no_enumeration\",
\"session_security\": \"none\", \"smb_encryption\": false,
\"smb_signing\": false, \"use_ldaps\": false, \"use_start_tls\": false },
\"svm\": { \"name\": \"vs1\", \"uuid\": \"e0c20d9c-96cd-11eb-97da-
0050568e684d\" }}"

# The response:
{
"num_records": 1,
"records": [
  {
    "svm": {
      "uuid": "e0c20d9c-96cd-11eb-97da-0050568e684d",
      "name": "vs1"
```

```
      },
      "name": "CIFS1",
      "ad_domain": {
        "fqdn": "ONTAPAVC.COM",
        "organizational_unit": "CN=Computers"
      },
      "enabled": true,
      "comment": "This CIFS Server Belongs to CS Department",
      "security": {
        "restrict_anonymous": "no_enumeration",
        "smb_signing": false,
        "smb_encryption": false,
        "kdc_encryption": false,
        "aes_netlogon_enabled": false,
        "try_ldap_channel_binding": false,
        "referral_enabled": false,
        "lm_compatibility_level": "lm_ntlm_ntlmv2_krb",
        "encrypt_dc_connection": false,
        "use_start_tls": false,
        "session_security": "none",
        "use_ldaps": false
      },
      "netbios": {
        "aliases": [
          "ALIAS_1",
          "ALIAS_2",
          "ALIAS_3"
        ],
        "wins_servers": [
          "10.224.65.20",
          "10.224.65.21"
        ],
        "enabled": false
      },
      "default_unix_user": "string",
      "options": {
        "advanced_sparse_file": true,
        "referral": false,
        "widelink_reparse_versions": [
          "smb1"
        ],
        "multichannel": true,
        "path_component_cache": true,
        "null_user_windows_name": "string",
        "junction_reparse": true,
        "fsctl_trim": true,
```

```
      "large_mtu": true,
      "fake_open": true,
      "smb_credits": 128,
      "admin_to_root_mapping": true,
      "copy_offload": true
    }
  }
],
"job": {
  "uuid": "825a0b4b-9703-11eb-8cc1-0050568e684d",
  "_links": {
    "self": {
      "href": "/api/cluster/jobs/825a0b4b-9703-11eb-8cc1-0050568e684d"
    }
  }
}
}
}
```

Creating a CIFS server when using AKV

```
# The API:
POST /api/protocols/cifs/services

# The call:
curl -X POST "https://<mgmt-
ip>/api/protocols/cifs/services?return_timeout=10&return_records=true" -H
"accept: application/json" -H "authorization: Basic <CREDENTIALS>" -H
"Content-Type: application/json" -d "{ \"key_vault_uri\":
\"https://testkv.vault.azure.net\", \"client_secret\": \"<CLIENT-SECRET-
ACCESS-KEY>\", \"authentication_method\": \"client_secret\",
\"tenant_id\": \"c9f32fcb-4ab7-40fe-af1b-1850d46cfbbe\", \"client_id\":
\"e959d1b5-5a63-4284-9268-851e30e3eceb\", \"ad_domain\": { \"fqdn\":
\"ontapavc.com\", \"organizational_unit\": \"CN=Computers\", \"user\":
\"administrator\" }, \"comment\": \"This CIFS Server Belongs to CS
Department\", \"default_unix_user\": \"string\", \"enabled\": true,
\"name\": \"CIFS1\", \"netbios\": { \"aliases\": [ \"ALIAS_1\",
\"ALIAS_2\", \"ALIAS_3\" ], \"enabled\": false, \"wins_servers\": [
\"10.224.65.20\", \"10.224.65.21\" ] }, \"options\": {
\"admin_to_root_mapping\": true, \"advanced_sparse_file\": true,
\"copy_offload\": true, \"fake_open\": true, \"fsctl_trim\": true,
\"junction_reparse\": true, \"large_mtu\": true, \"multichannel\": true,
\"null_user_windows_name\": \"string\", \"path_component_cache\": true,
```

```
\"referral\": false, \"smb_credits\": 128, \"widelink_reparse_versions\":
[ \"smb1\" ] }, \"security\": { \"encrypt_dc_connection\": false,
\"kdc_encryption\": false, \"restrict_anonymous\": \"no_enumeration\",
\"session_security\": \"none\", \"smb_encryption\": false,
\"smb_signing\": false, \"use_ldaps\": false, \"use_start_tls\": false },
\"svm\": { \"name\": \"vs1\", \"uuid\": \"e0c20d9c-96cd-11eb-97da-
0050568e684d\" }}"

# The response:
{
"num_records": 1,
"records": [
  {
    "svm": {
      "uuid": "e0c20d9c-96cd-11eb-97da-0050568e684d",
      "name": "vs1"
    },
    "name": "CIFS1",
    "ad_domain": {
      "fqdn": "ONTAPAVC.COM",
      "organizational_unit": "CN=Computers"
    },
    "enabled": true,
    "comment": "This CIFS Server Belongs to CS Department",
    "security": {
      "restrict_anonymous": "no_enumeration",
      "smb_signing": false,
      "smb_encryption": false,
      "kdc_encryption": false,
      "aes_netlogon_enabled": false,
      "try_ldap_channel_binding": false,
      "referral_enabled": false,
      "lm_compatibility_level": "lm_ntlm_ntlmv2_krb",
      "encrypt_dc_connection": false,
      "use_start_tls": false,
      "session_security": "none",
      "use_ldaps": false
    },
    "netbios": {
      "aliases": [
        "ALIAS_1",
        "ALIAS_2",
        "ALIAS_3"
      ],
      "wins_servers": [
        "10.224.65.20",
```

```
        "10.224.65.21"
      ],
      "enabled": false
    },
    "default_unix_user": "string",
    "options": {
      "advanced_sparse_file": true,
      "referral": false,
      "widelink_reparse_versions": [
        "smb1"
      ],
      "multichannel": true,
      "path_component_cache": true,
      "null_user_windows_name": "string",
      "junction_reparse": true,
      "fsctl_trim": true,
      "large_mtu": true,
      "fake_open": true,
      "smb_credits": 128,
      "admin_to_root_mapping": true,
      "copy_offload": true
    }
  }
],
"job": {
  "uuid": "825a0b4b-9703-11eb-8cc1-0050568e684d",
  "_links": {
    "self": {
      "href": "/api/cluster/jobs/825a0b4b-9703-11eb-8cc1-0050568e684d"
    }
  }
}
}
}
```

Creating a CIFS server for Hybrid user

```
# The API:
POST /api/protocols/cifs/services

# The call:
curl -X POST "https://<mgmt-
ip>/api/protocols/cifs/services?return_timeout=10&return_records=true" -H
"accept: application/json" -H "authorization: Basic <CREDENTIALS>" -H
"Content-Type: application/json" -d "{ \"auth_user_type\":
\"hybrid_user\", \"client_certificate\": \"certificate added to azure
application\", \"authentication_method\": \"certificate\", \"tenant_id\":
\"c9f32fcb-4ab7-40fe-af1b-1850d46cfbbe\", \"client_id\": \"e959d1b5-5a63-
4284-9268-851e30e3eceb\", \"ad_domain\": { \"fqdn\": \"ontapavc.com\",
\"organizational_unit\": \"CN=Computers\" }, \"comment\": \"This CIFS
Server Belongs to CS Department\", \"enabled\": true, \"name\": \"CIFS1\",
\"svm\": { \"name\": \"vs1\", \"uuid\": \"e0c20d9c-96cd-11eb-97da-
0050568e684d\" }}"

# The response:
{
"num_records": 1,
"records": [
  {
    "svm": {
      "uuid": "e0c20d9c-96cd-11eb-97da-0050568e684d",
      "name": "vs1"
    },
    "name": "CIFS1",
    "ad_domain": {
      "fqdn": "ONTAPAVC.COM",
      "organizational_unit": "CN=Computers"
    },
    "enabled": true,
    "comment": "This CIFS Server Belongs to CS Department",
  }
],
"job": {
  "uuid": "825a0b4b-9703-11eb-8cc1-0050568e684d",
  "_links": {
    "self": {
      "href": "/api/cluster/jobs/825a0b4b-9703-11eb-8cc1-0050568e684d"
    }
  }
}
}
```

Creating a CIFS server when using the security.advertised_kdc_encryptions field

```
# The API:
POST /api/protocols/cifs/services

# The call:
curl -X POST "https://<mgmt-
ip>/api/protocols/cifs/services?return_timeout=120&return_records=true&for
ce=true" -H "accept: application/json" -H "authorization: Basic
<CREDENTIALS>" -H "Content-Type: application/json" -d "{ \"ad_domain\": {
\"fqdn\": \"testdomain.com\", \"organizational_unit\": \"CN=Computers\",
\"password\": \"<PASSWORD-FOR-USER>\", \"user\": \"administrator\" },
\"enabled\": true, \"name\": \"CIFS_server1\", \"security\": {
\"advertised_kdc_encryptions\": [ \"aes-128\" ] }, \"svm\": { \"name\":
\"testvs\", \"uuid\": \"508375d4-fb16-11ee-a792-005056a75b5c\" }}"

# The response:
{
"num_records": 1,
"records": [
  {
    "svm": {
      "uuid": "508375d4-fb16-11ee-a792-005056a75b5c",
      "name": "testvs"
    },
    "name": "CIFS_SERVER1",
    "domain_workgroup": "TESTDOMAIN",
    "ad_domain": {
      "fqdn": "TESTDOMAIN.COM",
      "organizational_unit": "CN=Computers",
      "default_site": ""
    },
    "enabled": true,
    "comment": "",
    "security": {
      "restrict_anonymous": "no_enumeration",
      "smb_signing": false,
      "smb_encryption": false,
      "kdc_encryption": true,
      "lm_compatibility_level": "lm_ntlm_ntlmv2_krb",
      "aes_netlogon_enabled": false,
      "try_ldap_channel_binding": true,
      "ldap_referral_enabled": false,
      "advertised_kdc_encryptions": [
```

```
        "aes_128"
      ],
      "encrypt_dc_connection": false,
      "use_start_tls": false,
      "session_security": "none",
      "use_ldaps": false
    },
    "netbios": {
      "wins_servers": [],
      "enabled": false
    },
    "default_unix_user": "pcuser",
    "statistics": {
      "timestamp": "2024-04-16T15:17:41Z",
      "status": "ok",
      "throughput_raw": {
        "read": 0,
        "write": 0,
        "total": 0
      },
      "iops_raw": {
        "read": 0,
        "write": 0,
        "other": 0,
        "total": 0
      },
      "latency_raw": {
        "read": 0,
        "write": 0,
        "other": 0,
        "total": 0
      }
    },
    "options": {
      "advanced_sparse_file": true,
      "referral": false,
      "widelink_reparse_versions": [
        "smb1"
      ],
      "multichannel": false,
      "path_component_cache": true,
      "junction_reparse": true,
      "fsctl_trim": true,
      "large_mtu": true,
      "fake_open": true,
      "smb_credits": 512,
```

```
            "admin_to_root_mapping": true,
            "copy_offload": true,
            "shadowcopy": true,
            "shadowcopy_dir_depth": 5,
            "export_policy_enabled": false
        },
        "group_policy_object_enabled": false
    }
],
"job": {
    "uuid": "73eec230-fc04-11ee-a792-005056a75b5c",
    "_links": {
        "self": {
            "href": "/api/cluster/jobs/73eec230-fc04-11ee-a792-005056a75b5c"
        }
    }
}
}
}
```

Retrieving the full CIFS server configuration for all SVMs in the cluster

```
# The API:
GET /api/protocols/cifs/services

# The call:
curl -X GET "https://<mgmt-
ip>/api/protocols/cifs/services?fields=*&return_records=true&return_timeou
t=15" -H "accept: application/json" -H "authorization: Basic
<CREDENTIALS>"

# The response:
{
"records": [
    {
        "svm": {
            "uuid": "e0c20d9c-96cd-11eb-97da-0050568e684d",
            "name": "vs1"
        },
        "name": "CIFS1",
        "ad_domain": {
            "fqdn": "ONTAPAVC.COM",
            "organizational_unit": "CN=Computers"
```

```
      },
      "enabled": true,
      "comment": "This CIFS Server Belongs to CS Department",
      "security": {
        "restrict_anonymous": "no_enumeration",
        "smb_signing": false,
        "smb_encryption": false,
        "kdc_encryption": false,
        "aes_netlogon_enabled": false,
        "try_ldap_channel_binding": false,
        "referral_enabled": false,
        "lm_compatibility_level": "lm_ntlm_ntlmv2_krb",
        "encrypt_dc_connection": false,
        "use_start_tls": false,
        "session_security": "none",
        "use_ldaps": false
      },
      "netbios": {
        "aliases": [
          "ALIAS_1",
          "ALIAS_2",
          "ALIAS_3"
        ],
        "wins_servers": [
          "10.224.65.20",
          "10.224.65.21"
        ],
        "enabled": false
      },
      "default_unix_user": "string",
      "options": {
        "advanced_sparse_file": true,
        "referral": false,
        "widelink_reparse_versions": [
          "smb1"
        ],
        "multichannel": true,
        "path_component_cache": true,
        "null_user_windows_name": "string",
        "junction_reparse": true,
        "fsctl_trim": true,
        "large_mtu": true,
        "fake_open": true,
        "smb_credits": 128,
        "admin_to_root_mapping": true,
        "copy_offload": true
```

```
      }
    }
  ],
  "num_records": 1
}
```

Retrieving CIFS server configuration details for a specific SVM

```
# The API:
GET /api/protocols/cifs/services/{svm.uuid}

# The call:
curl -X GET "https://<mgmt-ip>/api/protocols/cifs/services/e0c20d9c-96cd-
11eb-97da-0050568e684d" -H "accept: application/json" -H "authorization:
Basic <CREDENTIALS>"

# The response:
{
"svm": {
  "uuid": "e0c20d9c-96cd-11eb-97da-0050568e684d",
  "name": "vs1"
},
"name": "CIFS1",
"ad_domain": {
  "fqdn": "ONTAPAVC.COM",
  "organizational_unit": "CN=Computers"
},
"enabled": true,
"comment": "This CIFS Server Belongs to CS Department",
"security": {
  "restrict_anonymous": "no_enumeration",
  "smb_signing": false,
  "smb_encryption": false,
  "kdc_encryption": false,
  "aes_netlogon_enabled": false,
  "try_ldap_channel_binding": false,
  "referral_enabled": false,
  "lm_compatibility_level": "lm_ntlm_ntlmv2_krb",
  "encrypt_dc_connection": false,
  "use_start_tls": false,
  "session_security": "none",
  "use_ldaps": false
```

```
  },
  "netbios": {
    "aliases": [
      "ALIAS_1",
      "ALIAS_2",
      "ALIAS_3"
    ],
    "wins_servers": [
      "10.224.65.20",
      "10.224.65.21"
    ],
    "enabled": false
  },
  "default_unix_user": "string",
  "options": {
    "advanced_sparse_file": true,
    "referral": false,
    "widelink_reparse_versions": [
      "smb1"
    ],
    "multichannel": true,
    "path_component_cache": true,
    "null_user_windows_name": "string",
    "junction_reparse": true,
    "fsctl_trim": true,
    "large_mtu": true,
    "fake_open": true,
    "smb_credits": 128,
    "admin_to_root_mapping": true,
    "copy_offload": true
  }
}
```

Updating CIFS server properties for the specified SVM

```
# The API:
PATCH /api/protocols/cifs/services/{svm.uuid}

# The call:
curl -X PATCH "https://<mgmt-ip>/api/protocols/cifs/services/e0c20d9c-
96cd-11eb-97da-0050568e684d" -H "accept: application/json" -H
"authorization: Basic <CREDENTIALS>" -H "Content-Type: application/json"
-d "{ \"comment\": \"CIFS SERVER MODIFICATION\"}"
```

Removing a CIFS server for a specific SVM

To delete a CIFS server, use the following API. This will delete the CIFS server along with other CIFS
configurations such as CIFS share, share ACLs, homedir search-path, and so on.

```
# The API:
DELETE /api/protocols/cifs/services/{svm.uuid}

# The call:
curl -X DELETE "https://<mgmt-ip>/api/protocols/cifs/services/e0c20d9c-
96cd-11eb-97da-0050568e684d" -H "accept: application/json" -H
"authorization: Basic <CREDENTIALS>" -H "Content-Type: application/json"
-d "{ \"ad_domain\": { \"fqdn\": \"ontapavc.com\",
\"organizational_unit\": \"CN=Computers\", \"password\": \"<PASSWORD-FOR-
USER>\", \"user\": \"administrator\" }, \"force\": true}"

# The call when using AKV:
curl -X DELETE "https://<mgmt-ip>/api/protocols/cifs/services/e0c20d9c-
96cd-11eb-97da-0050568e684d" -H "accept: application/json" -H
"authorization: Basic <CREDENTIALS>" -H "Content-Type: application/json"
-d "{ \"key_vault_uri\": \"https://testkv.vault.azure.net\",
\"client_secret\": \"<AWS-SECRET-ACCESS-KEY>\", \"authentication_method\":
\"client_secret\", \"tenant_id\": \"c9f32fcb-4ab7-40fe-af1b-
1850d46cfbbe\", \"client_id\": \"e959d1b5-5a63-4284-9268-851e30e3eceb\",
\"ad_domain\": { \"fqdn\": \"ontapavc.com\", \"organizational_unit\":
\"CN=Computers\" , \"user\": \"administrator\" }, \"force\": true}"

# The call when using EntraId:
curl -X DELETE "https://<mgmt-ip>/api/protocols/cifs/services/e0c20d9c-
96cd-11eb-97da-0050568e684d" -H "accept: application/json" -H
"authorization: Basic <CREDENTIALS>" -H "Content-Type: application/json"
-d "{ \"auth_user_type\": \"hybrid-user\", \"client_certificate\":
\"client_certificate_added_to_azure_application\",
\"authentication_method\": \"certificate\", \"tenant_id\": \"c9f32fcb-
4ab7-40fe-af1b-1850d46cfbbe\", \"client_id\": \"e959d1b5-5a63-4284-9268-
851e30e3eceb\", \"ad_domain\": { \"fqdn\": \"ontapavc.com\",
\"organizational_unit\": \"CN=Computers\"}, \"force\": true}"
```

Retrieve CIFS servers

GET `/protocols/cifs/services`

Introduced In: 9.6

Retrieves CIFS servers.

Expensive properties

There is an added computational cost to retrieving values for these properties. They are not included by default

in GET results and must be explicitly requested using the `fields` query parameter. See Requesting specific fields to learn more.

- `statistics.*`

- `metric.*`

Related ONTAP commands

- `vserver cifs server show`

- `vserver cifs server options show`

- `vserver cifs server security show`

Learn more

- DOC /protocols/cifs/services

Parameters

Name	Type	In	Required	Description
proxy_username	string	query	False	Filter by proxy_username - Introduced in: 9.15
auth_user_type	string	query	False	Filter by auth_user_type - Introduced in: 9.16
security.restrict_anonymous	string	query	False	Filter by security.restrict_anonymous
security.use_ldaps	boolean	query	False	Filter by security.use_ldaps - Introduced in: 9.10
security.smb_signing	boolean	query	False	Filter by security.smb_signing

Name	Type	In	Required	Description
security.ldap_referral _enabled	boolean	query	False	Filter by security.ldap_referra l_enabled • Introduced in: 9.10
security.kdc_encrypti on	boolean	query	False	Filter by security.kdc_encrypt ion
security.aes_netlogo n_enabled	boolean	query	False	Filter by security.aes_netlogo n_enabled • Introduced in: 9.10
security.session_sec urity	string	query	False	Filter by security.session_sec urity • Introduced in: 9.10
security.try_ldap_ch annel_binding	boolean	query	False	Filter by security.try_ldap_ch annel_binding • Introduced in: 9.10
security.use_start_tls	boolean	query	False	Filter by security.use_start_tl s • Introduced in: 9.10
security.lm_compati bility_level	string	query	False	Filter by security.lm_compati bility_level • Introduced in: 9.8

Name	Type	In	Required	Description
security.encrypt_dc_connection	boolean	query	False	Filter by security.encrypt_dc_connection • Introduced in: 9.8
security.smb_encryption	boolean	query	False	Filter by security.smb_encryption
security.advertised_kdc_encryptions	string	query	False	Filter by security.advertised_kdc_encryptions • Introduced in: 9.12
proxy_host	string	query	False	Filter by proxy_host • Introduced in: 9.15
client_id	string	query	False	Filter by client_id • Introduced in: 9.15
svm.name	string	query	False	Filter by svm.name
svm.uuid	string	query	False	Filter by svm.uuid
ad_domain.default_site	string	query	False	Filter by ad_domain.default_site • Introduced in: 9.13
ad_domain.fqdn	string	query	False	Filter by ad_domain.fqdn
ad_domain.organizational_unit	string	query	False	Filter by ad_domain.organizational_unit

Name	Type	In	Required	Description
workgroup	string	query	False	Filter by workgroup • Introduced in: 9.15 • maxLength: 15 • minLength: 1
tenant_id	string	query	False	Filter by tenant_id • Introduced in: 9.15
verify_host	boolean	query	False	Filter by verify_host • Introduced in: 9.15
oauth_host	string	query	False	Filter by oauth_host • Introduced in: 9.15
options.widelink_reparse_versions	string	query	False	Filter by options.widelink_reparse_versions • Introduced in: 9.10
options.shadowcopy	boolean	query	False	Filter by options.shadowcopy • Introduced in: 9.11
options.max_same_user_sessions_per_connection	integer	query	False	Filter by options.max_same_user_sessions_per_connection • Introduced in: 9.16

Name	Type	In	Required	Description
options.max_watches_set_per_tree	integer	query	False	Filter by options.max_watches_set_per_tree • Introduced in: 9.16
options.max_opens_same_file_per_tree	integer	query	False	Filter by options.max_opens_same_file_per_tree • Introduced in: 9.16
options.copy_offload	boolean	query	False	Filter by options.copy_offload • Introduced in: 9.10
options.fake_open	boolean	query	False	Filter by options.fake_open • Introduced in: 9.10
options.referral	boolean	query	False	Filter by options.referral • Introduced in: 9.10
options.max_same_tree_connect_per_session	integer	query	False	Filter by options.max_same_tree_connect_per_session • Introduced in: 9.16
options.smb_credits	integer	query	False	Filter by options.smb_credits • Introduced in: 9.10 • Max value: 8192 • Min value: 2

Name	Type	In	Required	Description
options.advanced_sparse_file	boolean	query	False	Filter by options.advanced_sparse_file • Introduced in: 9.10
options.dac_enabled	boolean	query	False	Filter by options.dac_enabled • Introduced in: 9.15
options.junction_reparse	boolean	query	False	Filter by options.junction_reparse • Introduced in: 9.10
options.shadowcopy_dir_depth	integer	query	False	Filter by options.shadowcopy_dir_depth • Introduced in: 9.11
options.multichannel	boolean	query	False	Filter by options.multichannel • Introduced in: 9.10
options.fsctl_trim	boolean	query	False	Filter by options.fsctl_trim • Introduced in: 9.10
options.trusted_domain_enum_search_enabled	boolean	query	False	Filter by options.trusted_domain_enum_search_enabled • Introduced in: 9.16

Name	Type	In	Required	Description
options.max_lifs_per_session	integer	query	False	Filter by options.max_lifs_per_session • Introduced in: 9.16 • Max value: 256 • Min value: 1
options.client_dup_detection_enabled	boolean	query	False	Filter by options.client_dup_detection_enabled • Introduced in: 9.16
options.path_component_cache	boolean	query	False	Filter by options.path_component_cache • Introduced in: 9.10
options.admin_to_root_mapping	boolean	query	False	Filter by options.admin_to_root_mapping • Introduced in: 9.10
options.client_version_reporting_enabled	boolean	query	False	Filter by options.client_version_reporting_enabled • Introduced in: 9.16
options.null_user_windows_name	string	query	False	Filter by options.null_user_windows_name • Introduced in: 9.10
options.large_mtu	boolean	query	False	Filter by options.large_mtu • Introduced in: 9.10

Name	Type	In	Required	Description
options.max_connections_per_session	integer	query	False	Filter by options.max_connections_per_session • Introduced in: 9.16 • Max value: 1024 • Min value: 2
options.backup_symlink_enabled	boolean	query	False	Filter by options.backup_symlink_enabled • Introduced in: 9.15
options.export_policy_enabled	boolean	query	False	Filter by options.export_policy_enabled • Introduced in: 9.13
proxy_type	string	query	False	Filter by proxy_type • Introduced in: 9.15
comment	string	query	False	Filter by comment • maxLength: 256 • minLength: 0
default_unix_user	string	query	False	Filter by default_unix_user
metric.iops.other	integer	query	False	Filter by metric.iops.other • Introduced in: 9.7
metric.iops.total	integer	query	False	Filter by metric.iops.total • Introduced in: 9.7

Name	Type	In	Required	Description
metric.iops.write	integer	query	False	Filter by metric.iops.write • Introduced in: 9.7
metric.iops.read	integer	query	False	Filter by metric.iops.read • Introduced in: 9.7
metric.latency.other	integer	query	False	Filter by metric.latency.other • Introduced in: 9.7
metric.latency.total	integer	query	False	Filter by metric.latency.total • Introduced in: 9.7
metric.latency.write	integer	query	False	Filter by metric.latency.write • Introduced in: 9.7
metric.latency.read	integer	query	False	Filter by metric.latency.read • Introduced in: 9.7
metric.timestamp	string	query	False	Filter by metric.timestamp • Introduced in: 9.7
metric.throughput.write	integer	query	False	Filter by metric.throughput.write • Introduced in: 9.7

Name	Type	In	Required	Description
metric.throughput.read	integer	query	False	Filter by metric.throughput.read • Introduced in: 9.7
metric.throughput.total	integer	query	False	Filter by metric.throughput.total • Introduced in: 9.7
metric.status	string	query	False	Filter by metric.status • Introduced in: 9.7
metric.duration	string	query	False	Filter by metric.duration • Introduced in: 9.7
authentication_method	string	query	False	Filter by authentication_method • Introduced in: 9.15
timeout	integer	query	False	Filter by timeout • Introduced in: 9.15
group_policy_object_enabled	boolean	query	False	Filter by group_policy_object_enabled • Introduced in: 9.12
netbios.enabled	boolean	query	False	Filter by netbios.enabled

Name	Type	In	Required	Description
netbios.wins_servers	string	query	False	Filter by netbios.wins_servers
netbios.aliases	string	query	False	Filter by netbios.aliases • maxLength: 15 • minLength: 1
auth-style	string	query	False	Filter by auth-style • Introduced in: 9.15
name	string	query	False	Filter by name • maxLength: 15 • minLength: 1
statistics.latency_raw.other	integer	query	False	Filter by statistics.latency_raw.other • Introduced in: 9.7
statistics.latency_raw.total	integer	query	False	Filter by statistics.latency_raw.total • Introduced in: 9.7
statistics.latency_raw.write	integer	query	False	Filter by statistics.latency_raw.write • Introduced in: 9.7
statistics.latency_raw.read	integer	query	False	Filter by statistics.latency_raw.read • Introduced in: 9.7

Name	Type	In	Required	Description
statistics.iops_raw.other	integer	query	False	Filter by statistics.iops_raw.other • Introduced in: 9.7
statistics.iops_raw.total	integer	query	False	Filter by statistics.iops_raw.total • Introduced in: 9.7
statistics.iops_raw.write	integer	query	False	Filter by statistics.iops_raw.write • Introduced in: 9.7
statistics.iops_raw.read	integer	query	False	Filter by statistics.iops_raw.read • Introduced in: 9.7
statistics.status	string	query	False	Filter by statistics.status • Introduced in: 9.7
statistics.throughput_raw.write	integer	query	False	Filter by statistics.throughput_raw.write • Introduced in: 9.7
statistics.throughput_raw.read	integer	query	False	Filter by statistics.throughput_raw.read • Introduced in: 9.7

Name	Type	In	Required	Description
statistics.throughput _raw.total	integer	query	False	Filter by statistics.throughput _raw.total • Introduced in: 9.7
statistics.timestamp	string	query	False	Filter by statistics.timestamp • Introduced in: 9.7
proxy_port	integer	query	False	Filter by proxy_port • Introduced in: 9.15
enabled	boolean	query	False	Filter by enabled
key_vault_uri	string	query	False	Filter by key_vault_uri • Introduced in: 9.15
fields	array[string]	query	False	Specify the fields to return.
max_records	integer	query	False	Limit the number of records returned.
return_records	boolean	query	False	The default is true for GET calls. When set to false, only the number of records is returned. • Default value: 1

Name	Type	In	Required	Description
return_timeout	integer	query	False	The number of seconds to allow the call to execute before returning. When iterating over a collection, the default is 15 seconds. ONTAP returns earlier if either max records or the end of the collection is reached. • Max value: 120 • Min value: 0 • Default value: 15
order_by	array[string]	query	False	Order results by specified fields and optional [asc

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
num_records	integer	Number of records
records	array[cifs_service]	

```json
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "ad_domain": {
        "default_site": "string",
        "fqdn": "example.com",
        "organizational_unit": "string"
      },
      "auth-style": "domain",
      "auth_user_type": "string",
      "authentication_method": "string",
      "client_id": "e959d1b5-5a63-4284-9268-851e30e3eceb",
      "comment": "This CIFS Server Belongs to CS Department",
      "default_unix_user": "string",
      "key_vault_uri": "https://kmip-akv-keyvault.vault.azure.net/",
      "metric": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "duration": "PT15S",
        "iops": {
          "read": 200,
          "total": 1000,
          "write": 100
        },
        "latency": {
          "read": 200,
          "total": 1000,
```

```
          "write": 100
        },
        "status": "ok",
        "throughput": {
          "read": 200,
          "total": 1000,
          "write": 100
        },
        "timestamp": "2017-01-25 11:20:13 +0000"
      },
      "name": "CIFS1",
      "netbios": {
        "aliases": [
          "ALIAS_1",
          "ALIAS_2",
          "ALIAS_3"
        ],
        "wins_servers": [
          "10.224.65.20",
          "10.224.65.21"
        ]
      },
      "oauth_host": "login.microsoftonline.com",
      "options": {
        "max_connections_per_session": 32,
        "max_lifs_per_session": 256,
        "max_opens_same_file_per_tree": 1000,
        "max_same_tree_connect_per_session": 5000,
        "max_same_user_sessions_per_connection": 2500,
        "max_watches_set_per_tree": 500,
        "null_user_windows_name": "string",
        "smb_credits": 128,
        "widelink_reparse_versions": [
          "smb1"
        ]
      },
      "proxy_host": "proxy.eng.com",
      "proxy_port": 1234,
      "proxy_type": "string",
      "proxy_username": "proxyuser",
      "security": {
        "advertised_kdc_encryptions": [
          "string"
        ],
        "lm_compatibility_level": "string",
        "restrict_anonymous": "string",
```

```
          "session_security": "string"
        },
        "statistics": {
          "iops_raw": {
            "read": 200,
            "total": 1000,
            "write": 100
          },
          "latency_raw": {
            "read": 200,
            "total": 1000,
            "write": 100
          },
          "status": "ok",
          "throughput_raw": {
            "read": 200,
            "total": 1000,
            "write": 100
          },
          "timestamp": "2017-01-25 11:20:13 +0000"
        },
        "svm": {
          "_links": {
            "self": {
              "href": "/api/resourcelink"
            }
          },
          "name": "svm1",
          "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
        },
        "tenant_id": "c9f32fcb-4ab7-40fe-af1b-1850d46cfbbe",
        "timeout": 25,
        "workgroup": "workgrp1"
    }
  ]
}
```

Error

Status: Default, Error

Name	Type	Description
error	returned_error	

Example error

```json
{
  "error": {
    "arguments": [
      {
        "code": "string",
        "message": "string"
      }
    ],
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
next	href	
self	href	

_links

Name	Type	Description
self	href	

ad_domain

Name	Type	Description
default_site	string	The default site used by LIFs that do not have a site membership.
fqdn	string	The fully qualified domain name of the Windows Active Directory to which this CIFS server belongs. A CIFS server appears as a member of Windows server object in the Active Directory store. POST and PATCH only.
organizational_unit	string	Specifies the organizational unit within the Active Directory domain to associate with the CIFS server. POST and PATCH only.

iops

The rate of I/O operations observed at the storage object.

Name	Type	Description
other	integer	Performance metric for other I/O operations. Other I/O operations can be metadata operations, such as directory lookups and so on.
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

latency

The round trip latency in microseconds observed at the storage object.

Name	Type	Description
other	integer	Performance metric for other I/O operations. Other I/O operations can be metadata operations, such as directory lookups and so on.
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

throughput

The rate of throughput bytes per second observed at the storage object.

Name	Type	Description
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.

Name	Type	Description
write	integer	Performance metric for write I/O operations.

metric

Performance numbers, such as IOPS latency and throughput, for SVM protocols.

Name	Type	Description
_links	_links	
duration	string	The duration over which this sample is calculated. The time durations are represented in the ISO-8601 standard format. Samples can be calculated over the following durations:
iops	iops	The rate of I/O operations observed at the storage object.
latency	latency	The round trip latency in microseconds observed at the storage object.
status	string	Any errors associated with the sample. For example, if the aggregation of data over multiple nodes fails then any of the partial errors might be returned, "ok" on success, or "error" on any internal uncategorized failure. Whenever a sample collection is missed but done at a later time, it is back filled to the previous 15 second timestamp and tagged with "backfilled_data". "Inconsistent_delta_time" is encountered when the time between two collections is not the same for all nodes. Therefore, the aggregated value might be over or under inflated. "Negative_delta" is returned when an expected monotonically increasing value has decreased in value. "Inconsistent_old_data" is returned when one or more nodes do not have the latest data.

Name	Type	Description
throughput	throughput	The rate of throughput bytes per second observed at the storage object.
timestamp	string	The timestamp of the performance data.

cifs_netbios

Name	Type	Description
aliases	array[string]	
enabled	boolean	Specifies whether NetBios name service (NBNS) is enabled for the CIFS. If this service is enabled, the CIFS server will start sending the broadcast for name registration.
wins_servers	array[string]	

cifs_service_options

Name	Type	Description
admin_to_root_mapping	boolean	Specifies whether or not Administrator can be mapped to the UNIX user "root".
advanced_sparse_file	boolean	Specifies whether or not the CIFS server supports the advanced sparse file capabilities. This allows CIFS clients to query the allocated ranges of a file and to write zeroes or free data blocks for ranges of a file.
backup_symlink_enabled	boolean	Specifies whether or not to preserve UNIX symlinks during backup through SMB.
client_dup_detection_enabled	boolean	Specifies whether or not client duplicate session detection is enabled for CIFS.
client_version_reporting_enabled	boolean	Specifies whether or not client version reporting is enabled for CIFS.

Name	Type	Description
copy_offload	boolean	Specifies whether or not to enable the Copy Offload feature. This feature enables direct data transfers within or between compatible storage devices without transferring the data through the host computer. Note that this will also enable/disable the direct copy feature accordingly.
dac_enabled	boolean	Specifies whether or not the Dynamic Access Control (DAC) feature is enabled for the CIFS server.
export_policy_enabled	boolean	Specifies whether or not export policies are enabled for CIFS.
fake_open	boolean	Specifies whether or not fake open support is enabled. This parameter allows you to optimize the open and close requests coming from SMB 2 clients.
fsctl_trim	boolean	Specifies whether or not the trim requests (FSCTL_FILE_LEVEL_TRIM) are supported on the CIFS server.
junction_reparse	boolean	Specifies whether or not the reparse point support is enabled. When enabled the CIFS server exposes junction points to Windows clients as reparse points. This parameter is only active if the client has negotiated use of the SMB 2 or SMB 3 protocol. This parameter is not supported for SVMs with Infinite Volume.
large_mtu	boolean	Specifies whether or not SMB clients can send reads up to 1 MB in size.

Name	Type	Description
max_connections_per_session	integer	Specifies the maximum number of connections allowed per multichannel session.
max_lifs_per_session	integer	Specifies the maximum number of LIFs advertised per multichannel session.
max_opens_same_file_per_tree	integer	Specifies the maximum number of opens on the same file per tree.
max_same_tree_connect_per_session	integer	Specifies the maximum number of same tree connections per session.
max_same_user_sessions_per_connection	integer	Specifies the maximum number of same user sessions per connection.
max_watches_set_per_tree	integer	Specifies the maximum number of watches set per tree.
multichannel	boolean	Specifies whether or not the CIFS server supports Multichannel.
null_user_windows_name	string	Specifies a Windows User or Group name that should be mapped in case of a NULL user value.
path_component_cache	boolean	Specifies whether or not the path component cache is enabled on the CIFS server.
referral	boolean	Specifies whether or not to refer clients to more optimal LIFs. When enabled, it automatically refers clients to a data LIF local to the node which hosts the root of the requested share.

Name	Type	Description
shadowcopy	boolean	Specifies whether or not to enable the Shadowcopy Feature. This feature enables to take share-based backup copies of data that is in a data-consistent state at a specific point in time where the data is accessed over SMB 3.0 shares.
shadowcopy_dir_depth	integer	Specifies the maximum level of subdirectories on which ONTAP should create shadow copies. • Default value: 5 • Introduced in: 9.11 • x-nullable: true
smb_credits	integer	Specifies the maximum number of outstanding requests on a CIFS connection.
trusted_domain_enum_search_enabled	boolean	Specifies whether or not to enable trusted domain search. • If this parameter is set to true, it displays CIFS options only for CIFS servers that support enumeration of bidirectional trusted domains and that support searching in all bidirectional trusted domains when performing Windows user lookups for UNIX user to Windows user name mapping. • If set to false, it displays CIFS options for CIFS servers that do not support enumeration of bidirectional trusted domains.
widelink_reparse_versions	array[string]	Specifies the CIFS protocol versions for which the widelink is reported as reparse point.

cifs_service_security

Name	Type	Description
advertised_kdc_encryptions	array[string]	
aes_netlogon_enabled	boolean	Specifies whether or not an AES session key is enabled for the Netlogon channel.
encrypt_dc_connection	boolean	Specifies whether encryption is required for domain controller connections.

Name	Type	Description
kdc_encryption	boolean	This attribute has been deprecated. Use "security.advertised_kdc_encryptions" to specify the encryption type to use. Specifies whether AES-128 and AES-256 encryption is enabled for all Kerberos-based communication with the Active Directory KDC. To take advantage of the strongest security with Kerberos-based communication, AES-256 and AES-128 encryption can be enabled on the CIFS server. Kerberos-related communication for CIFS is used during CIFS server creation on the SVM, as well as during the SMB session setup phase. The CIFS server supports the following encryption types for Kerberos communication:

• RC4-HMAC

• DES

• AES When the CIFS server is created, the domain controller creates a computer machine account in Active Directory. After a newly created machine account authenticates, the KDC and the CIFS server negotiates encryption types. At this time, the KDC becomes aware of the encryption capabilities of the particular machine account and uses those

Name	Type	Description
ldap_referral_enabled	boolean	Specifies whether or not LDAP referral chasing is enabled for AD LDAP connections.
lm_compatibility_level	string	It is CIFS server minimum security level, also known as the LMCompatibilityLevel. The minimum security level is the minimum level of the security tokens that the CIFS server accepts from SMB clients. The available values are: • lm_ntlm_ntlmv2_krb Accepts LM, NTLM, NTLMv2 and Kerberos • ntlm_ntlmv2_krb Accepts NTLM, NTLMv2 and Kerberos • ntlmv2_krb Accepts NTLMv2 and Kerberos • krb Accepts Kerberos only
restrict_anonymous	string	Specifies what level of access an anonymous user is granted. An anonymous user (also known as a "null user") can list or enumerate certain types of system information from Windows hosts on the network, including user names and details, account policies, and share names. Access for the anonymous user can be controlled by specifying one of three access restriction settings. The available values are: • no_restriction - No access restriction for an anonymous user. • no_enumeration - Enumeration is restricted for an anonymous user. • no_access - All access is restricted for an anonymous user.

Name	Type	Description
session_security	string	Specifies client session security for AD LDAP connections. The available values are: • none - No Signing or Sealing. • sign - Sign LDAP traffic. • seal - Seal and Sign LDAP traffic
smb_encryption	boolean	Specifies whether encryption is required for incoming CIFS traffic.
smb_signing	boolean	Specifies whether signing is required for incoming CIFS traffic. SMB signing helps to ensure that network traffic between the CIFS server and the client is not compromised.
try_ldap_channel_binding	boolean	Specifies whether or not channel binding is attempted in the case of TLS/LDAPS.
use_ldaps	boolean	Specifies whether or not to use use LDAPS for secure Active Directory LDAP connections by using the TLS/SSL protocols.
use_start_tls	boolean	Specifies whether or not to use SSL/TLS for allowing secure LDAP communication with Active Directory LDAP servers.

iops_raw

The number of I/O operations observed at the storage object. This should be used along with delta time to calculate the rate of I/O operations per unit of time.

Name	Type	Description
other	integer	Performance metric for other I/O operations. Other I/O operations can be metadata operations, such as directory lookups and so on.

Name	Type	Description
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

latency_raw

The raw latency in microseconds observed at the storage object. This should be divided by the raw IOPS value to calculate the average latency per I/O operation.

Name	Type	Description
other	integer	Performance metric for other I/O operations. Other I/O operations can be metadata operations, such as directory lookups and so on.
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

throughput_raw

Throughput bytes observed at the storage object. This should be used along with delta time to calculate the rate of throughput bytes per unit of time.

Name	Type	Description
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

statistics

These are raw performance numbers, such as IOPS latency and throughput for SVM protocols. These numbers are aggregated across all nodes in the cluster and increase with the uptime of the cluster.

Name	Type	Description
iops_raw	iops_raw	The number of I/O operations observed at the storage object. This should be used along with delta time to calculate the rate of I/O operations per unit of time.
latency_raw	latency_raw	The raw latency in microseconds observed at the storage object. This should be divided by the raw IOPS value to calculate the average latency per I/O operation.
status	string	Any errors associated with the sample. For example, if the aggregation of data over multiple nodes fails then any of the partial errors might be returned, "ok" on success, or "error" on any internal uncategorized failure. Whenever a sample collection is missed but done at a later time, it is back filled to the previous 15 second timestamp and tagged with "backfilled_data". "Inconsistent_delta_time" is encountered when the time between two collections is not the same for all nodes. Therefore, the aggregated value might be over or under inflated. "Negative_delta" is returned when an expected monotonically increasing value has decreased in value. "Inconsistent_old_data" is returned when one or more nodes do not have the latest data.
throughput_raw	throughput_raw	Throughput bytes observed at the storage object. This should be used along with delta time to calculate the rate of throughput bytes per unit of time.

Name	Type	Description
timestamp	string	The timestamp of the performance data.

svm

SVM, applies only to SVM-scoped objects.

Name	Type	Description
_links	_links	
name	string	The name of the SVM. This field cannot be specified in a PATCH method.
uuid	string	The unique identifier of the SVM. This field cannot be specified in a PATCH method.

cifs_service

Name	Type	Description
_links	_links	
ad_domain	ad_domain	
auth-style	string	Authentication type.
auth_user_type	string	Specifies the type of user who can access the SMB Volume. The default is domain_user. In the case of a hybrid-user, ONTAP won't contact on-premise ADDS. • enum: ["domain_user", "hybrid_user"] • Introduced in: 9.16 • x-nullable: true
authentication_method	string	Specifies the authentication method. The available values are: • client_secret • certificate

Name	Type	Description
client_id	string	Application client ID of the deployed Azure application with appropriate access to an AKV or EntraId.
comment	string	A descriptive text comment for the CIFS server. SMB clients can see the CIFS server comment when browsing servers on the network. If there is a space in the comment, you must enclose the entire string in quotation marks.
default_unix_user	string	Specifies the UNIX user to which any authenticated CIFS user is mapped to, if the normal user mapping rules fails.
enabled	boolean	Specifies if the CIFS service is administratively enabled.
group_policy_object_enabled	boolean	If set to true, group policies will be applied to the SVM.
key_vault_uri	string	URI of the deployed AKV that is used by ONTAP for storing keys. • example: https://kmip-akv-keyvault.vault.azure.net/ • format: uri • Introduced in: 9.15 • x-nullable: true
metric	metric	Performance numbers, such as IOPS latency and throughput, for SVM protocols.
name	string	The name of the CIFS server.
netbios	cifs_netbios	
oauth_host	string	Open authorization server host name.
options	cifs_service_options	
proxy_host	string	Proxy host.

Name	Type	Description
proxy_port	integer	Proxy port.
proxy_type	string	Proxy type.
proxy_username	string	Proxy username.
security	cifs_service_security	
statistics	statistics	These are raw performance numbers, such as IOPS latency and throughput for SVM protocols. These numbers are aggregated across all nodes in the cluster and increase with the uptime of the cluster.
svm	svm	SVM, applies only to SVM-scoped objects.
tenant_id	string	Directory (tenant) ID of the deployed Azure application with appropriate access to an AKV or EntraId.
timeout	integer	AKV connection timeout, in seconds. The allowed range is between 0 to 30 seconds.
verify_host	boolean	Verify the identity of the AKV host name. By default, verify_host is set to true.
workgroup	string	The workgroup name.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments

Name	Type	Description
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Create a CIFS server

POST `/protocols/cifs/services`

Introduced In: 9.6

Creates a CIFS server. Each SVM can have one CIFS server.

Important notes

- The CIFS server name might or might not be the same as the SVM name.
- The CIFS server name can contain up to 15 characters.
- The CIFS server name does not support the following characters: @ # * ( ) = + [ ] \| ; : " , < > / ?

Required properties when creating CIFS server with Windows Active Directory domain

- `svm.uuid` or `svm.name` - Existing SVM in which to create the CIFS server.
- `name` - Name of the CIFS server.
- `ad_domain.fqdn` - Fully qualified domain name of the Windows Active Directory to which this CIFS server belongs.
- `ad_domain.user` - User account with the access to add the CIFS server to the Active Directory.
- `ad_domain.password` - Account password used to add this CIFS server to the Active Directory.

Required properties when creating CIFS server in Workgroup mode

- `svm.uuid` or `svm.name` - Existing SVM in which to create the CIFS server.
- `name` - Name of the CIFS server.
- `workgroup` - Name of the workgroup to which this CIFS server belongs.

Required properties when using AKV for authentication (ANF platform)

- `svm.uuid` or `svm.name` - Existing SVM in which to create the CIFS server.
- `name` - Name of the CIFS server.
- `ad_domain.user` - User account with the access to add the CIFS server to the Active Directory.

- `ad_domain.fqdn` - Fully qualified domain name of the Windows Active Directory to which this CIFS server belongs.

- `client_id` - Application client ID of the deployed Azure application with appropriate access to an AKV or EntraId.

- `tenant_id` - Directory (tenant) ID of the deployed Azure application with appropriate access to an AKV or EntraId.

- `key_vault_uri` - URI of the deployed AKV that is used by ONTAP for storing keys.

- `authentication_method` - Authentication method used by the application to prove its identity to AKV or EntraId. It can be either "client_secret" or "certificate".

- `auth_user_type` - Type of user who can access the SMB Volume. It can be either "domain_user" or "hybrid_user". The default is domain_user. In the case of a hybrid-user, ONTAP cannot access on-premise ADDS.

- `client_secret` - Secret used by the application to prove its identity to AKV.

- `client_certificate` - Base64 encoded PKCS12 certificate used by the application to prove its identity to AKV.

Recommended optional properties

- `comment` - Add a text comment of up to 256 characters about the CIFS server.

- `netbios.aliases` - Add a comma-delimited list of one or more NetBIOS aliases for the CIFS server.

- `netbios.wins_servers` - Add a list of Windows Internet Name Server (WINS) addresses that manage and map the NetBIOS name of the CIFS server to their network IP addresses. The IP addresses must be IPv4 addresses.

Default property values

If not specified in POST, the following default property values are assigned:

- `ad_domain.organizational_unit` - *CN=Computers*

- `enabled` - *true*

- `security.restrict_anonymous` - *no_enumeration*

- `security.smb_signing` - *false*

- `security.smb_encryption` - *false*

- `security.encrypt_dc_connection` - *false*

- `default_unix_user` - *pcuser*

- `netbios.enabled` - *false* However, if either "netbios.wins-server" or "netbios.aliases" is set during POST and if `netbios.enabled` is not specified then `netbios.enabled` is set to true.

- `security.aes_netlogon_enabled` - *false*

- `security.try_ldap_channel_binding` - *true*

- `security.ldap_referral_enabled` - *false*

Related ONTAP commands

- `vserver cifs server create`

- `vserver cifs server options modify`

- `vserver cifs security modify`

- `vserver cifs server add-netbios-aliases`

Learn more

- DOC /protocols/cifs/services

Parameters

Name	Type	In	Required	Description
force	boolean	query	False	If this is set and a machine account with the same name as specified in 'cifs-server name' exists in the Active Directory, existing machine account will be overwritten and reused. • Introduced in: 9.11

Name	Type	In	Required	Description
return_timeout	integer	query	False	The number of seconds to allow the call to execute before returning. When doing a POST, PATCH, or DELETE operation on a single record, the default is 0 seconds. This means that if an asynchronous operation is started, the server immediately returns HTTP code 202 (Accepted) along with a link to the job. If a non-zero value is specified for POST, PATCH, or DELETE operations, ONTAP waits that length of time to see if the job completes so it can return something other than 202. • Default value: 0 • Max value: 120 • Min value: 0
return_records	boolean	query	False	The default is false. If set to true, the records are returned. • Default value:

Request Body

Name	Type	Description
ad_domain	ad_domain	
auth-style	string	Authentication type.

Name	Type	Description
auth_user_type	string	Specifies the type of user who can access the SMB Volume. The default is domain_user. In the case of a hybrid-user, ONTAP won't contact on-premise ADDS. • enum: ["domain_user", "hybrid_user"] • Introduced in: 9.16 • x-nullable: true
authentication_method	string	Specifies the authentication method. The available values are: • client_secret • certificate
client_certificate	string	PKCS12 certificate used by the application to prove its identity to AKV.
client_id	string	Application client ID of the deployed Azure application with appropriate access to an AKV or EntraId.
client_secret	string	Secret used by the application to prove its identity to AKV.
comment	string	A descriptive text comment for the CIFS server. SMB clients can see the CIFS server comment when browsing servers on the network. If there is a space in the comment, you must enclose the entire string in quotation marks.
default_unix_user	string	Specifies the UNIX user to which any authenticated CIFS user is mapped to, if the normal user mapping rules fails.
enabled	boolean	Specifies if the CIFS service is administratively enabled.

Name	Type	Description
key_vault_uri	string	URI of the deployed AKV that is used by ONTAP for storing keys. • example: https://kmip-akv-keyvault.vault.azure.net/ • format: uri • Introduced in: 9.15 • x-nullable: true
name	string	The name of the CIFS server.
netbios	cifs_netbios	
oauth_host	string	Open authorization server host name.
options	cifs_service_options	
proxy_host	string	Proxy host.
proxy_password	string	Proxy password. Password is not audited.
proxy_port	integer	Proxy port.
proxy_type	string	Proxy type.
proxy_username	string	Proxy username.
security	cifs_service_security	
svm	svm	SVM, applies only to SVM-scoped objects.
tenant_id	string	Directory (tenant) ID of the deployed Azure application with appropriate access to an AKV or EntraId.
timeout	integer	AKV connection timeout, in seconds. The allowed range is between 0 to 30 seconds.
verify_host	boolean	Verify the identity of the AKV host name. By default, verify_host is set to true.

Name	Type	Description
workgroup	string	The workgroup name.

Example request

```json
{
  "ad_domain": {
    "default_site": "string",
    "fqdn": "example.com",
    "organizational_unit": "string",
    "password": "string",
    "user": "string"
  },
  "auth-style": "domain",
  "auth_user_type": "string",
  "authentication_method": "string",
  "client_certificate": "PEM Cert",
  "client_id": "e959d1b5-5a63-4284-9268-851e30e3eceb",
  "client_secret": "<APPLICATION-CLIENT-SECRET-FOR-AKV>",
  "comment": "This CIFS Server Belongs to CS Department",
  "default_unix_user": "string",
  "group_policy_object_enabled": true,
  "key_vault_uri": "https://kmip-akv-keyvault.vault.azure.net/",
  "name": "CIFS1",
  "netbios": {
    "aliases": [
      "ALIAS_1",
      "ALIAS_2",
      "ALIAS_3"
    ],
    "wins_servers": [
      "10.224.65.20",
      "10.224.65.21"
    ]
  },
  "oauth_host": "login.microsoftonline.com",
  "options": {
    "max_connections_per_session": 32,
    "max_lifs_per_session": 256,
    "max_opens_same_file_per_tree": 1000,
    "max_same_tree_connect_per_session": 5000,
    "max_same_user_sessions_per_connection": 2500,
    "max_watches_set_per_tree": 500,
    "null_user_windows_name": "string",
    "smb_credits": 128,
    "widelink_reparse_versions": [
      "smb1"
    ]
  },
```

```
      "proxy_host": "proxy.eng.com",
      "proxy_password": "proxypassword",
      "proxy_port": 1234,
      "proxy_type": "string",
      "proxy_username": "proxyuser",
      "security": {
        "advertised_kdc_encryptions": [
          "string"
        ],
        "restrict_anonymous": "string",
        "session_security": "string"
      },
      "svm": {
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
      },
      "tenant_id": "c9f32fcb-4ab7-40fe-af1b-1850d46cfbbe",
      "timeout": 25,
      "workgroup": "workgrp1"
    }
```

Response

```
Status: 202, Accepted
```

Name	Type	Description
job	job_link	

Example response

```
{
  "job": {
    "uuid": "string"
  }
}
```

Headers

Name	Description	Type
Location	Useful for tracking the resource location	string

Response

```
Status: 201, Created
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
1115127	The cluster lacks a valid CIFS license.
3735751	Failed to authenticate and retrieve the access token from the Azure OAuth host.
3735752	Failed to extract the private key from the Azure Key Vault certificate.
3735753	Unsupported content_type in the Azure secrets response.
3735754	Failed to parse the JSON response from Azure Key Vault.
3735755	REST API call to Azure failed.
3735756	Invalid client certificate.
3735757	Failed to generate client assertion.
3735762	The provided Azure Key Vault configuration is incorrect.
3735763	The provided Azure Key Vault configuration is incomplete.
3735764	Request to Azure failed. Reason - Azure error code and Azure error message.
655388	Failed to create the CIFS server. Failure can occur due to multiple reasons. For example: STARTTLS and LDAPS cannot be used together or a password update failed or error from LDAP server or Kerberos Error: KDC has no support for encryption type.
655524	CIFS server creation failed.
655538	CIFS server creation failed because a server with the same name already exists.
655562	NetBIOS name is longer than 15 characters.
655563	NetBIOS name contains characters that are not allowed.

Error Code	Description
655771	The number of NetBIOS aliases cannot exceed the maximum supported number of '200'.
655914	Failed to create the Active Directory machine account.
655923	Retrieving credentials from AKV is not supported because the effective cluster version is not ONTAP 9.15.0 or later.
656464	Failed to create the Active Directory machine account. Reason: Invalid Credentials.
656465	Failed to create the Active Directory machine account. Reason: Account with same name already exists.
656466	Failed to create the Active Directory machine account. Reason: Domain Controller is not reachable or does not exist.
656467	Failed to create the Active Directory machine account. Reason: Organizational-Unit not found.
656473	Fields security.kdc_encryption and security.advertised_kdc_encryptions are mutually exclusive. Specify only one of the two.
655477	Only one CIFS server is supported per SVM.
656487	Missing fields when doing CIFS operation with hybrid auth user type.

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

ad_domain

Name	Type	Description
default_site	string	The default site used by LIFs that do not have a site membership.
fqdn	string	The fully qualified domain name of the Windows Active Directory to which this CIFS server belongs. A CIFS server appears as a member of Windows server object in the Active Directory store. POST and PATCH only.
organizational_unit	string	Specifies the organizational unit within the Active Directory domain to associate with the CIFS server. POST and PATCH only.
password	string	The account password used to add this CIFS server to the Active Directory. This is not audited.
user	string	The user account used to add this CIFS server to the Active Directory.

iops

The rate of I/O operations observed at the storage object.

Name	Type	Description
other	integer	Performance metric for other I/O operations. Other I/O operations can be metadata operations, such as directory lookups and so on.

Name	Type	Description
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

latency

The round trip latency in microseconds observed at the storage object.

Name	Type	Description
other	integer	Performance metric for other I/O operations. Other I/O operations can be metadata operations, such as directory lookups and so on.
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

throughput

The rate of throughput bytes per second observed at the storage object.

Name	Type	Description
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

metric

Performance numbers, such as IOPS latency and throughput, for SVM protocols.

Name	Type	Description
duration	string	The duration over which this sample is calculated. The time durations are represented in the ISO-8601 standard format. Samples can be calculated over the following durations:
iops	iops	The rate of I/O operations observed at the storage object.
latency	latency	The round trip latency in microseconds observed at the storage object.
status	string	Any errors associated with the sample. For example, if the aggregation of data over multiple nodes fails then any of the partial errors might be returned, "ok" on success, or "error" on any internal uncategorized failure. Whenever a sample collection is missed but done at a later time, it is back filled to the previous 15 second timestamp and tagged with "backfilled_data". "Inconsistent_ delta_time" is encountered when the time between two collections is not the same for all nodes. Therefore, the aggregated value might be over or under inflated. "Negative_delta" is returned when an expected monotonically increasing value has decreased in value. "Inconsistent_old_data" is returned when one or more nodes do not have the latest data.
throughput	throughput	The rate of throughput bytes per second observed at the storage object.
timestamp	string	The timestamp of the performance data.

cifs_netbios

Name	Type	Description
aliases	array[string]	
enabled	boolean	Specifies whether NetBios name service (NBNS) is enabled for the CIFS. If this service is enabled, the CIFS server will start sending the broadcast for name registration.
wins_servers	array[string]	

cifs_service_options

Name	Type	Description
admin_to_root_mapping	boolean	Specifies whether or not Administrator can be mapped to the UNIX user "root".
advanced_sparse_file	boolean	Specifies whether or not the CIFS server supports the advanced sparse file capabilities. This allows CIFS clients to query the allocated ranges of a file and to write zeroes or free data blocks for ranges of a file.
backup_symlink_enabled	boolean	Specifies whether or not to preserve UNIX symlinks during backup through SMB.
client_dup_detection_enabled	boolean	Specifies whether or not client duplicate session detection is enabled for CIFS.
client_version_reporting_enabled	boolean	Specifies whether or not client version reporting is enabled for CIFS.

Name	Type	Description
copy_offload	boolean	Specifies whether or not to enable the Copy Offload feature. This feature enables direct data transfers within or between compatible storage devices without transferring the data through the host computer. Note that this will also enable/disable the direct copy feature accordingly.
dac_enabled	boolean	Specifies whether or not the Dynamic Access Control (DAC) feature is enabled for the CIFS server.
export_policy_enabled	boolean	Specifies whether or not export policies are enabled for CIFS.
fake_open	boolean	Specifies whether or not fake open support is enabled. This parameter allows you to optimize the open and close requests coming from SMB 2 clients.
fsctl_trim	boolean	Specifies whether or not the trim requests (FSCTL_FILE_LEVEL_TRIM) are supported on the CIFS server.
junction_reparse	boolean	Specifies whether or not the reparse point support is enabled. When enabled the CIFS server exposes junction points to Windows clients as reparse points. This parameter is only active if the client has negotiated use of the SMB 2 or SMB 3 protocol. This parameter is not supported for SVMs with Infinite Volume.
large_mtu	boolean	Specifies whether or not SMB clients can send reads up to 1 MB in size.

Name	Type	Description
max_connections_per_session	integer	Specifies the maximum number of connections allowed per multichannel session.
max_lifs_per_session	integer	Specifies the maximum number of LIFs advertised per multichannel session.
max_opens_same_file_per_tree	integer	Specifies the maximum number of opens on the same file per tree.
max_same_tree_connect_per_session	integer	Specifies the maximum number of same tree connections per session.
max_same_user_sessions_per_connection	integer	Specifies the maximum number of same user sessions per connection.
max_watches_set_per_tree	integer	Specifies the maximum number of watches set per tree.
multichannel	boolean	Specifies whether or not the CIFS server supports Multichannel.
null_user_windows_name	string	Specifies a Windows User or Group name that should be mapped in case of a NULL user value.
path_component_cache	boolean	Specifies whether or not the path component cache is enabled on the CIFS server.
referral	boolean	Specifies whether or not to refer clients to more optimal LIFs. When enabled, it automatically refers clients to a data LIF local to the node which hosts the root of the requested share.

Name	Type	Description
shadowcopy	boolean	Specifies whether or not to enable the Shadowcopy Feature. This feature enables to take share-based backup copies of data that is in a data-consistent state at a specific point in time where the data is accessed over SMB 3.0 shares.
shadowcopy_dir_depth	integer	Specifies the maximum level of subdirectories on which ONTAP should create shadow copies. • Default value: 5 • Introduced in: 9.11 • x-nullable: true
smb_credits	integer	Specifies the maximum number of outstanding requests on a CIFS connection.
trusted_domain_enum_search_enabled	boolean	Specifies whether or not to enable trusted domain search. • If this parameter is set to true, it displays CIFS options only for CIFS servers that support enumeration of bidirectional trusted domains and that support searching in all bidirectional trusted domains when performing Windows user lookups for UNIX user to Windows user name mapping. • If set to false, it displays CIFS options for CIFS servers that do not support enumeration of bidirectional trusted domains.
widelink_reparse_versions	array[string]	Specifies the CIFS protocol versions for which the widelink is reported as reparse point.

cifs_service_security

Name	Type	Description
advertised_kdc_encryptions	array[string]	
aes_netlogon_enabled	boolean	Specifies whether or not an AES session key is enabled for the Netlogon channel.
encrypt_dc_connection	boolean	Specifies whether encryption is required for domain controller connections.

Name	Type	Description
kdc_encryption	boolean	This attribute has been deprecated. Use "security.advertised_kdc_encryptions" to specify the encryption type to use. Specifies whether AES-128 and AES-256 encryption is enabled for all Kerberos-based communication with the Active Directory KDC. To take advantage of the strongest security with Kerberos-based communication, AES-256 and AES-128 encryption can be enabled on the CIFS server. Kerberos-related communication for CIFS is used during CIFS server creation on the SVM, as well as during the SMB session setup phase. The CIFS server supports the following encryption types for Kerberos communication: • RC4-HMAC • DES • AES When the CIFS server is created, the domain controller creates a computer machine account in Active Directory. After a newly created machine account authenticates, the KDC and the CIFS server negotiates encryption types. At this time, the KDC becomes aware of the encryption capabilities of the particular machine account and uses those

Name	Type	Description
ldap_referral_enabled	boolean	Specifies whether or not LDAP referral chasing is enabled for AD LDAP connections.
restrict_anonymous	string	Specifies what level of access an anonymous user is granted. An anonymous user (also known as a "null user") can list or enumerate certain types of system information from Windows hosts on the network, including user names and details, account policies, and share names. Access for the anonymous user can be controlled by specifying one of three access restriction settings. The available values are: • no_restriction - No access restriction for an anonymous user. • no_enumeration - Enumeration is restricted for an anonymous user. • no_access - All access is restricted for an anonymous user.
session_security	string	Specifies client session security for AD LDAP connections. The available values are: • none - No Signing or Sealing. • sign - Sign LDAP traffic. • seal - Seal and Sign LDAP traffic
smb_encryption	boolean	Specifies whether encryption is required for incoming CIFS traffic.
smb_signing	boolean	Specifies whether signing is required for incoming CIFS traffic. SMB signing helps to ensure that network traffic between the CIFS server and the client is not compromised.

Name	Type	Description
try_ldap_channel_binding	boolean	Specifies whether or not channel binding is attempted in the case of TLS/LDAPS.
use_ldaps	boolean	Specifies whether or not to use use LDAPS for secure Active Directory LDAP connections by using the TLS/SSL protocols.
use_start_tls	boolean	Specifies whether or not to use SSL/TLS for allowing secure LDAP communication with Active Directory LDAP servers.

iops_raw

The number of I/O operations observed at the storage object. This should be used along with delta time to calculate the rate of I/O operations per unit of time.

Name	Type	Description
other	integer	Performance metric for other I/O operations. Other I/O operations can be metadata operations, such as directory lookups and so on.
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

latency_raw

The raw latency in microseconds observed at the storage object. This should be divided by the raw IOPS value to calculate the average latency per I/O operation.

Name	Type	Description
other	integer	Performance metric for other I/O operations. Other I/O operations can be metadata operations, such as directory lookups and so on.

Name	Type	Description
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

throughput_raw

Throughput bytes observed at the storage object. This should be used along with delta time to calculate the rate of throughput bytes per unit of time.

Name	Type	Description
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

statistics

These are raw performance numbers, such as IOPS latency and throughput for SVM protocols. These numbers are aggregated across all nodes in the cluster and increase with the uptime of the cluster.

Name	Type	Description
iops_raw	iops_raw	The number of I/O operations observed at the storage object. This should be used along with delta time to calculate the rate of I/O operations per unit of time.
latency_raw	latency_raw	The raw latency in microseconds observed at the storage object. This should be divided by the raw IOPS value to calculate the average latency per I/O operation.

Name	Type	Description
status	string	Any errors associated with the sample. For example, if the aggregation of data over multiple nodes fails then any of the partial errors might be returned, "ok" on success, or "error" on any internal uncategorized failure. Whenever a sample collection is missed but done at a later time, it is back filled to the previous 15 second timestamp and tagged with "backfilled_data". "Inconsistent_delta_time" is encountered when the time between two collections is not the same for all nodes. Therefore, the aggregated value might be over or under inflated. "Negative_delta" is returned when an expected monotonically increasing value has decreased in value. "Inconsistent_old_data" is returned when one or more nodes do not have the latest data.
throughput_raw	throughput_raw	Throughput bytes observed at the storage object. This should be used along with delta time to calculate the rate of throughput bytes per unit of time.
timestamp	string	The timestamp of the performance data.

svm

SVM, applies only to SVM-scoped objects.

Name	Type	Description
name	string	The name of the SVM. This field cannot be specified in a PATCH method.
uuid	string	The unique identifier of the SVM. This field cannot be specified in a PATCH method.

cifs_service

Name	Type	Description
ad_domain	ad_domain	
auth-style	string	Authentication type.
auth_user_type	string	Specifies the type of user who can access the SMB Volume. The default is domain_user. In the case of a hybrid-user, ONTAP won't contact on-premise ADDS. • enum: ["domain_user", "hybrid_user"] • Introduced in: 9.16 • x-nullable: true
authentication_method	string	Specifies the authentication method. The available values are: • client_secret • certificate
client_certificate	string	PKCS12 certificate used by the application to prove its identity to AKV.
client_id	string	Application client ID of the deployed Azure application with appropriate access to an AKV or EntraId.
client_secret	string	Secret used by the application to prove its identity to AKV.
comment	string	A descriptive text comment for the CIFS server. SMB clients can see the CIFS server comment when browsing servers on the network. If there is a space in the comment, you must enclose the entire string in quotation marks.
default_unix_user	string	Specifies the UNIX user to which any authenticated CIFS user is mapped to, if the normal user mapping rules fails.

Name	Type	Description
enabled	boolean	Specifies if the CIFS service is administratively enabled.
key_vault_uri	string	URI of the deployed AKV that is used by ONTAP for storing keys. • example: https://kmip-akv-keyvault.vault.azure.net/ • format: uri • Introduced in: 9.15 • x-nullable: true
name	string	The name of the CIFS server.
netbios	cifs_netbios	
oauth_host	string	Open authorization server host name.
options	cifs_service_options	
proxy_host	string	Proxy host.
proxy_password	string	Proxy password. Password is not audited.
proxy_port	integer	Proxy port.
proxy_type	string	Proxy type.
proxy_username	string	Proxy username.
security	cifs_service_security	
svm	svm	SVM, applies only to SVM-scoped objects.
tenant_id	string	Directory (tenant) ID of the deployed Azure application with appropriate access to an AKV or EntraId.
timeout	integer	AKV connection timeout, in seconds. The allowed range is between 0 to 30 seconds.

Name	Type	Description
verify_host	boolean	Verify the identity of the AKV host name. By default, verify_host is set to true.
workgroup	string	The workgroup name.

job_link

Name	Type	Description
uuid	string	The UUID of the asynchronous job that is triggered by a POST, PATCH, or DELETE operation.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Delete a CIFS server and related configurations

DELETE `/protocols/cifs/services/{svm.uuid}`

Introduced In: 9.6

Deletes a CIFS server and related CIFS configurations.

Important notes:

- The default value for the "force" field is false.

- If the "force" field is set along with user login credentials, the local CIFS configuration will be deleted irrespective of any communication errors.

- If the "force" field alone is set without passing the user login credentials, the local CIFS configuration will be deleted by not making any request to Active Directory.

Related ONTAP commands

- `vserver cifs server delete`

- `vserver cifs remove-netbios-aliases`

Learn more

- DOC /protocols/cifs/services

Parameters

Name	Type	In	Required	Description
force	boolean	query	False	When set, the local CIFS configuration is deleted irrespective of any communication errors. Default value for this field is false. • Introduced in: 9.11

Name	Type	In	Required	Description
return_timeout	integer	query	False	The number of seconds to allow the call to execute before returning. When doing a POST, PATCH, or DELETE operation on a single record, the default is 0 seconds. This means that if an asynchronous operation is started, the server immediately returns HTTP code 202 (Accepted) along with a link to the job. If a non-zero value is specified for POST, PATCH, or DELETE operations, ONTAP waits that length of time to see if the job completes so it can return something other than 202. • Default value: 0 • Max value: 120 • Min value: 0
svm.uuid	string	path	True	UUID of the SVM to which this object belongs.

Request Body

Name	Type	Description
ad_domain	ad_domain_delete	

Name	Type	Description
auth_user_type	string	Specifies the type of user who can access the SMB Volume. The default is domain_user. In the case of a hybrid-user, ONTAP won't contact on-premise ADDS. • enum: ["domain_user", "hybrid_user"] • Introduced in: 9.16 • x-nullable: true
authentication_method	string	Specifies the authentication method. The available values are: • client_secret • certificate
client_certificate	string	PKCS12 certificate used by the application to prove its identity to AKV.
client_id	string	Application client ID of the deployed Azure application with appropriate access to an AKV or EntraId.
client_secret	string	Secret used by the application to prove its identity to AKV.
key_vault_uri	string	URI of the deployed AKV that is used by ONTAP for storing keys. • example: https://kmip-akv-keyvault.vault.azure.net/ • format: uri • Introduced in: 9.15 • x-nullable: true
oauth_host	string	Open authorization server host name.
proxy_host	string	Proxy host.
proxy_password	string	Proxy password. Password is not audited.

Name	Type	Description
proxy_port	integer	Proxy port.
proxy_type	string	Proxy type.
proxy_username	string	Proxy username.
tenant_id	string	Directory (tenant) ID of the deployed Azure application with appropriate access to an AKV or EntraId.
timeout	integer	AKV connection timeout, in seconds. The allowed range is between 0 to 30 seconds.
verify_host	boolean	Verify the identity of the AKV host name. By default, verify_host is set to true.
workgroup	string	The workgroup name.

Example request

```json
{
  "ad_domain": {
    "fqdn": "example.com",
    "organizational_unit": "string",
    "password": "string",
    "user": "string"
  },
  "auth_user_type": "string",
  "authentication_method": "string",
  "client_certificate": "PEM Cert",
  "client_id": "e959d1b5-5a63-4284-9268-851e30e3eceb",
  "client_secret": "<APPLICATION-CLIENT-SECRET-FOR-AKV>",
  "key_vault_uri": "https://kmip-akv-keyvault.vault.azure.net/",
  "oauth_host": "login.microsoftonline.com",
  "proxy_host": "proxy.eng.com",
  "proxy_password": "proxypassword",
  "proxy_port": 1234,
  "proxy_type": "string",
  "proxy_username": "proxyuser",
  "tenant_id": "c9f32fcb-4ab7-40fe-af1b-1850d46cfbbe",
  "timeout": 25,
  "workgroup": "workgrp1"
}
```

Response

```
Status: 200, Ok
```

Name	Type	Description
job	job_link	

Example response

```json
{
  "job": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "uuid": "string"
  }
}
```

Response

```
Status: 202, Accepted
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
655525	In order to delete an Active Directory machine account for the CIFS server, you must supply the name and password of a Windows account with sufficient privileges.
3735751	Failed to authenticate and retrieve the access token from the Azure OAuth host.
3735752	Failed to extract the private key from the Azure Key Vault certificate.
3735753	Unsupported content_type in the Azure secrets response.
3735754	Failed to parse the JSON response from Azure Key Vault.
3735755	REST API call to Azure failed.
3735756	Invalid client certificate.
3735757	Failed to generate client assertion.

Error Code	Description
3735762	The provided Azure Key Vault configuration is incorrect.
3735763	The provided Azure Key Vault configuration is incomplete.
3735764	Request to Azure failed. Reason - Azure error code and Azure error message.
655563	NetBIOS name contains characters that are not allowed.
655562	NetBIOS name is longer than 15 characters.
655923	Retrieving credentials from AKV is not supported because the effective cluster version is not ONTAP 9.15.0 or later.
656487	Missing fields when doing CIFS operation with hybrid auth user type.

Name	Type	Description
error	returned_error	

Example error

```
{
  "error": {
    "arguments": [
      {
        "code": "string",
        "message": "string"
      }
    ],
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```

Definitions

See Definitions

ad_domain_delete

Name	Type	Description
fqdn	string	The fully qualified domain name of the Windows Active Directory to which this CIFS server belongs. A CIFS server appears as a member of Windows server object in the Active Directory store. POST and PATCH only.
organizational_unit	string	Specifies the organizational unit within the Active Directory domain to associate with the CIFS server. POST and PATCH only.
password	string	The account password used to add this CIFS server to the Active Directory. This is not audited.
user	string	The user account used to add this CIFS server to the Active Directory.

cifs_service_delete

Name	Type	Description
ad_domain	ad_domain_delete	
auth_user_type	string	Specifies the type of user who can access the SMB Volume. The default is domain_user. In the case of a hybrid-user, ONTAP won't contact on-premise ADDS. • enum: ["domain_user", "hybrid_user"] • Introduced in: 9.16 • x-nullable: true
authentication_method	string	Specifies the authentication method. The available values are: • client_secret • certificate

Name	Type	Description
client_certificate	string	PKCS12 certificate used by the application to prove its identity to AKV.
client_id	string	Application client ID of the deployed Azure application with appropriate access to an AKV or EntraId.
client_secret	string	Secret used by the application to prove its identity to AKV.
key_vault_uri	string	URI of the deployed AKV that is used by ONTAP for storing keys. • example: https://kmip-akv-keyvault.vault.azure.net/ • format: uri • Introduced in: 9.15 • x-nullable: true
oauth_host	string	Open authorization server host name.
proxy_host	string	Proxy host.
proxy_password	string	Proxy password. Password is not audited.
proxy_port	integer	Proxy port.
proxy_type	string	Proxy type.
proxy_username	string	Proxy username.
tenant_id	string	Directory (tenant) ID of the deployed Azure application with appropriate access to an AKV or EntraId.
timeout	integer	AKV connection timeout, in seconds. The allowed range is between 0 to 30 seconds.

Name	Type	Description
verify_host	boolean	Verify the identity of the AKV host name. By default, verify_host is set to true.
workgroup	string	The workgroup name.

href

Name	Type	Description
href	string	

_links

Name	Type	Description
self	href	

job_link

Name	Type	Description
_links	_links	
uuid	string	The UUID of the asynchronous job that is triggered by a POST, PATCH, or DELETE operation.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message

Name	Type	Description
target	string	The target parameter that caused the error.

Retrieve a CIFS server

GET `/protocols/cifs/services/{svm.uuid}`

Introduced In: 9.6

Retrieves a CIFS server.

Related ONTAP commands

- `vserver cifs server show`
- `vserver cifs server options show`
- `vserver cifs server security show`

Learn more

- DOC /protocols/cifs/services

Parameters

Name	Type	In	Required	Description
svm.uuid	string	path	True	
fields	array[string]	query	False	Specify the fields to return.

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
ad_domain	ad_domain	
auth-style	string	Authentication type.

Name	Type	Description
auth_user_type	string	Specifies the type of user who can access the SMB Volume. The default is domain_user. In the case of a hybrid-user, ONTAP won't contact on-premise ADDS. • enum: ["domain_user", "hybrid_user"] • Introduced in: 9.16 • x-nullable: true
authentication_method	string	Specifies the authentication method. The available values are: • client_secret • certificate
client_id	string	Application client ID of the deployed Azure application with appropriate access to an AKV or EntraId.
comment	string	A descriptive text comment for the CIFS server. SMB clients can see the CIFS server comment when browsing servers on the network. If there is a space in the comment, you must enclose the entire string in quotation marks.
default_unix_user	string	Specifies the UNIX user to which any authenticated CIFS user is mapped to, if the normal user mapping rules fails.
enabled	boolean	Specifies if the CIFS service is administratively enabled.
group_policy_object_enabled	boolean	If set to true, group policies will be applied to the SVM.

Name	Type	Description
key_vault_uri	string	URI of the deployed AKV that is used by ONTAP for storing keys. • example: https://kmip-akv-keyvault.vault.azure.net/ • format: uri • Introduced in: 9.15 • x-nullable: true
metric	metric	Performance numbers, such as IOPS latency and throughput, for SVM protocols.
name	string	The name of the CIFS server.
netbios	cifs_netbios	
oauth_host	string	Open authorization server host name.
options	cifs_service_options	
proxy_host	string	Proxy host.
proxy_port	integer	Proxy port.
proxy_type	string	Proxy type.
proxy_username	string	Proxy username.
security	cifs_service_security	
statistics	statistics	These are raw performance numbers, such as IOPS latency and throughput for SVM protocols. These numbers are aggregated across all nodes in the cluster and increase with the uptime of the cluster.
svm	svm	SVM, applies only to SVM-scoped objects.
tenant_id	string	Directory (tenant) ID of the deployed Azure application with appropriate access to an AKV or EntraId.

Name	Type	Description
timeout	integer	AKV connection timeout, in seconds. The allowed range is between 0 to 30 seconds.
verify_host	boolean	Verify the identity of the AKV host name. By default, verify_host is set to true.
workgroup	string	The workgroup name.

Example response

```json
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "ad_domain": {
    "default_site": "string",
    "fqdn": "example.com",
    "organizational_unit": "string"
  },
  "auth-style": "domain",
  "auth_user_type": "string",
  "authentication_method": "string",
  "client_id": "e959d1b5-5a63-4284-9268-851e30e3eceb",
  "comment": "This CIFS Server Belongs to CS Department",
  "default_unix_user": "string",
  "key_vault_uri": "https://kmip-akv-keyvault.vault.azure.net/",
  "metric": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "duration": "PT15S",
    "iops": {
      "read": 200,
      "total": 1000,
      "write": 100
    },
    "latency": {
      "read": 200,
      "total": 1000,
      "write": 100
    },
    "status": "ok",
    "throughput": {
      "read": 200,
      "total": 1000,
      "write": 100
    },
    "timestamp": "2017-01-25 11:20:13 +0000"
  },
  "name": "CIFS1",
```

```json
    "netbios": {
      "aliases": [
        "ALIAS_1",
        "ALIAS_2",
        "ALIAS_3"
      ],
      "wins_servers": [
        "10.224.65.20",
        "10.224.65.21"
      ]
    },
    "oauth_host": "login.microsoftonline.com",
    "options": {
      "max_connections_per_session": 32,
      "max_lifs_per_session": 256,
      "max_opens_same_file_per_tree": 1000,
      "max_same_tree_connect_per_session": 5000,
      "max_same_user_sessions_per_connection": 2500,
      "max_watches_set_per_tree": 500,
      "null_user_windows_name": "string",
      "smb_credits": 128,
      "widelink_reparse_versions": [
        "smb1"
      ]
    },
    "proxy_host": "proxy.eng.com",
    "proxy_port": 1234,
    "proxy_type": "string",
    "proxy_username": "proxyuser",
    "security": {
      "advertised_kdc_encryptions": [
        "string"
      ],
      "lm_compatibility_level": "string",
      "restrict_anonymous": "string",
      "session_security": "string"
    },
    "statistics": {
      "iops_raw": {
        "read": 200,
        "total": 1000,
        "write": 100
      },
      "latency_raw": {
        "read": 200,
        "total": 1000,
```

```
      "write": 100
    },
    "status": "ok",
    "throughput_raw": {
      "read": 200,
      "total": 1000,
      "write": 100
    },
    "timestamp": "2017-01-25 11:20:13 +0000"
  },
  "svm": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "tenant_id": "c9f32fcb-4ab7-40fe-af1b-1850d46cfbbe",
  "timeout": 25,
  "workgroup": "workgrp1"
}
```

Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error

```
{
  "error": {
    "arguments": [
      {
        "code": "string",
        "message": "string"
      }
    ],
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
self	href	

ad_domain

Name	Type	Description
default_site	string	The default site used by LIFs that do not have a site membership.
fqdn	string	The fully qualified domain name of the Windows Active Directory to which this CIFS server belongs. A CIFS server appears as a member of Windows server object in the Active Directory store. POST and PATCH only.
organizational_unit	string	Specifies the organizational unit within the Active Directory domain to associate with the CIFS server. POST and PATCH only.

iops

The rate of I/O operations observed at the storage object.

Name	Type	Description
other	integer	Performance metric for other I/O operations. Other I/O operations can be metadata operations, such as directory lookups and so on.
read	integer	Performance metric for read I/O operations.

Name	Type	Description
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

latency

The round trip latency in microseconds observed at the storage object.

Name	Type	Description
other	integer	Performance metric for other I/O operations. Other I/O operations can be metadata operations, such as directory lookups and so on.
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

throughput

The rate of throughput bytes per second observed at the storage object.

Name	Type	Description
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

metric

Performance numbers, such as IOPS latency and throughput, for SVM protocols.

Name	Type	Description
_links	_links	
duration	string	The duration over which this sample is calculated. The time durations are represented in the ISO-8601 standard format. Samples can be calculated over the following durations:
iops	iops	The rate of I/O operations observed at the storage object.
latency	latency	The round trip latency in microseconds observed at the storage object.
status	string	Any errors associated with the sample. For example, if the aggregation of data over multiple nodes fails then any of the partial errors might be returned, "ok" on success, or "error" on any internal uncategorized failure. Whenever a sample collection is missed but done at a later time, it is back filled to the previous 15 second timestamp and tagged with "backfilled_data". "Inconsistent_delta_time" is encountered when the time between two collections is not the same for all nodes. Therefore, the aggregated value might be over or under inflated. "Negative_delta" is returned when an expected monotonically increasing value has decreased in value. "Inconsistent_old_data" is returned when one or more nodes do not have the latest data.
throughput	throughput	The rate of throughput bytes per second observed at the storage object.
timestamp	string	The timestamp of the performance data.

cifs_netbios

Name	Type	Description
aliases	array[string]	
enabled	boolean	Specifies whether NetBios name service (NBNS) is enabled for the CIFS. If this service is enabled, the CIFS server will start sending the broadcast for name registration.
wins_servers	array[string]	

cifs_service_options

Name	Type	Description
admin_to_root_mapping	boolean	Specifies whether or not Administrator can be mapped to the UNIX user "root".
advanced_sparse_file	boolean	Specifies whether or not the CIFS server supports the advanced sparse file capabilities. This allows CIFS clients to query the allocated ranges of a file and to write zeroes or free data blocks for ranges of a file.
backup_symlink_enabled	boolean	Specifies whether or not to preserve UNIX symlinks during backup through SMB.
client_dup_detection_enabled	boolean	Specifies whether or not client duplicate session detection is enabled for CIFS.
client_version_reporting_enabled	boolean	Specifies whether or not client version reporting is enabled for CIFS.

Name	Type	Description
copy_offload	boolean	Specifies whether or not to enable the Copy Offload feature. This feature enables direct data transfers within or between compatible storage devices without transferring the data through the host computer. Note that this will also enable/disable the direct copy feature accordingly.
dac_enabled	boolean	Specifies whether or not the Dynamic Access Control (DAC) feature is enabled for the CIFS server.
export_policy_enabled	boolean	Specifies whether or not export policies are enabled for CIFS.
fake_open	boolean	Specifies whether or not fake open support is enabled. This parameter allows you to optimize the open and close requests coming from SMB 2 clients.
fsctl_trim	boolean	Specifies whether or not the trim requests (FSCTL_FILE_LEVEL_TRIM) are supported on the CIFS server.
junction_reparse	boolean	Specifies whether or not the reparse point support is enabled. When enabled the CIFS server exposes junction points to Windows clients as reparse points. This parameter is only active if the client has negotiated use of the SMB 2 or SMB 3 protocol. This parameter is not supported for SVMs with Infinite Volume.
large_mtu	boolean	Specifies whether or not SMB clients can send reads up to 1 MB in size.

Name	Type	Description
max_connections_per_session	integer	Specifies the maximum number of connections allowed per multichannel session.
max_lifs_per_session	integer	Specifies the maximum number of LIFs advertised per multichannel session.
max_opens_same_file_per_tree	integer	Specifies the maximum number of opens on the same file per tree.
max_same_tree_connect_per_session	integer	Specifies the maximum number of same tree connections per session.
max_same_user_sessions_per_connection	integer	Specifies the maximum number of same user sessions per connection.
max_watches_set_per_tree	integer	Specifies the maximum number of watches set per tree.
multichannel	boolean	Specifies whether or not the CIFS server supports Multichannel.
null_user_windows_name	string	Specifies a Windows User or Group name that should be mapped in case of a NULL user value.
path_component_cache	boolean	Specifies whether or not the path component cache is enabled on the CIFS server.
referral	boolean	Specifies whether or not to refer clients to more optimal LIFs. When enabled, it automatically refers clients to a data LIF local to the node which hosts the root of the requested share.

Name	Type	Description
shadowcopy	boolean	Specifies whether or not to enable the Shadowcopy Feature. This feature enables to take share-based backup copies of data that is in a data-consistent state at a specific point in time where the data is accessed over SMB 3.0 shares.
shadowcopy_dir_depth	integer	Specifies the maximum level of subdirectories on which ONTAP should create shadow copies. • Default value: 5 • Introduced in: 9.11 • x-nullable: true
smb_credits	integer	Specifies the maximum number of outstanding requests on a CIFS connection.
trusted_domain_enum_search_enabled	boolean	Specifies whether or not to enable trusted domain search. • If this parameter is set to true, it displays CIFS options only for CIFS servers that support enumeration of bidirectional trusted domains and that support searching in all bidirectional trusted domains when performing Windows user lookups for UNIX user to Windows user name mapping. • If set to false, it displays CIFS options for CIFS servers that do not support enumeration of bidirectional trusted domains.
widelink_reparse_versions	array[string]	Specifies the CIFS protocol versions for which the widelink is reported as reparse point.

cifs_service_security

Name	Type	Description
advertised_kdc_encryptions	array[string]	
aes_netlogon_enabled	boolean	Specifies whether or not an AES session key is enabled for the Netlogon channel.
encrypt_dc_connection	boolean	Specifies whether encryption is required for domain controller connections.

Name	Type	Description
kdc_encryption	boolean	(i) This attribute has been deprecated. Use "security.advertised_kdc_encryptions" to specify the encryption type to use. Specifies whether AES-128 and AES-256 encryption is enabled for all Kerberos-based communication with the Active Directory KDC. To take advantage of the strongest security with Kerberos-based communication, AES-256 and AES-128 encryption can be enabled on the CIFS server. Kerberos-related communication for CIFS is used during CIFS server creation on the SVM, as well as during the SMB session setup phase. The CIFS server supports the following encryption types for Kerberos communication:

• RC4-HMAC

• DES

• AES When the CIFS server is created, the domain controller creates a computer machine account in Active Directory. After a newly created machine account authenticates, the KDC and the CIFS server negotiates encryption types. At this time, the KDC becomes aware of the encryption capabilities of the particular machine account and uses those

Name	Type	Description
ldap_referral_enabled	boolean	Specifies whether or not LDAP referral chasing is enabled for AD LDAP connections.
lm_compatibility_level	string	It is CIFS server minimum security level, also known as the LMCompatibilityLevel. The minimum security level is the minimum level of the security tokens that the CIFS server accepts from SMB clients. The available values are: • lm_ntlm_ntlmv2_krb Accepts LM, NTLM, NTLMv2 and Kerberos • ntlm_ntlmv2_krb Accepts NTLM, NTLMv2 and Kerberos • ntlmv2_krb Accepts NTLMv2 and Kerberos • krb Accepts Kerberos only
restrict_anonymous	string	Specifies what level of access an anonymous user is granted. An anonymous user (also known as a "null user") can list or enumerate certain types of system information from Windows hosts on the network, including user names and details, account policies, and share names. Access for the anonymous user can be controlled by specifying one of three access restriction settings. The available values are: • no_restriction - No access restriction for an anonymous user. • no_enumeration - Enumeration is restricted for an anonymous user. • no_access - All access is restricted for an anonymous user.

Name	Type	Description
session_security	string	Specifies client session security for AD LDAP connections. The available values are: • none - No Signing or Sealing. • sign - Sign LDAP traffic. • seal - Seal and Sign LDAP traffic
smb_encryption	boolean	Specifies whether encryption is required for incoming CIFS traffic.
smb_signing	boolean	Specifies whether signing is required for incoming CIFS traffic. SMB signing helps to ensure that network traffic between the CIFS server and the client is not compromised.
try_ldap_channel_binding	boolean	Specifies whether or not channel binding is attempted in the case of TLS/LDAPS.
use_ldaps	boolean	Specifies whether or not to use use LDAPS for secure Active Directory LDAP connections by using the TLS/SSL protocols.
use_start_tls	boolean	Specifies whether or not to use SSL/TLS for allowing secure LDAP communication with Active Directory LDAP servers.

iops_raw

The number of I/O operations observed at the storage object. This should be used along with delta time to calculate the rate of I/O operations per unit of time.

Name	Type	Description
other	integer	Performance metric for other I/O operations. Other I/O operations can be metadata operations, such as directory lookups and so on.

Name	Type	Description
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

latency_raw

The raw latency in microseconds observed at the storage object. This should be divided by the raw IOPS value to calculate the average latency per I/O operation.

Name	Type	Description
other	integer	Performance metric for other I/O operations. Other I/O operations can be metadata operations, such as directory lookups and so on.
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

throughput_raw

Throughput bytes observed at the storage object. This should be used along with delta time to calculate the rate of throughput bytes per unit of time.

Name	Type	Description
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

statistics

These are raw performance numbers, such as IOPS latency and throughput for SVM protocols. These numbers are aggregated across all nodes in the cluster and increase with the uptime of the cluster.

Name	Type	Description
iops_raw	iops_raw	The number of I/O operations observed at the storage object. This should be used along with delta time to calculate the rate of I/O operations per unit of time.
latency_raw	latency_raw	The raw latency in microseconds observed at the storage object. This should be divided by the raw IOPS value to calculate the average latency per I/O operation.
status	string	Any errors associated with the sample. For example, if the aggregation of data over multiple nodes fails then any of the partial errors might be returned, "ok" on success, or "error" on any internal uncategorized failure. Whenever a sample collection is missed but done at a later time, it is back filled to the previous 15 second timestamp and tagged with "backfilled_data". "Inconsistent_delta_time" is encountered when the time between two collections is not the same for all nodes. Therefore, the aggregated value might be over or under inflated. "Negative_delta" is returned when an expected monotonically increasing value has decreased in value. "Inconsistent_old_data" is returned when one or more nodes do not have the latest data.
throughput_raw	throughput_raw	Throughput bytes observed at the storage object. This should be used along with delta time to calculate the rate of throughput bytes per unit of time.

Name	Type	Description
timestamp	string	The timestamp of the performance data.

svm

SVM, applies only to SVM-scoped objects.

Name	Type	Description
_links	_links	
name	string	The name of the SVM. This field cannot be specified in a PATCH method.
uuid	string	The unique identifier of the SVM. This field cannot be specified in a PATCH method.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Update CIFS mandatory and optional parameters

PATCH /protocols/cifs/services/{svm.uuid}

Introduced In: 9.6

Updates both the mandatory and optional parameters of the CIFS configuration. Ensure the CIFS server is administratively disabled when renaming the CIFS server or modifying the *ad_domain* properties.

Related ONTAP commands

- `vserver cifs server modify`

- `vserver cifs server options modify`

- `vserver cifs security modify`

- `vserver cifs server add-netbios-aliases`

- `vserver cifs server remove-netbios-aliases`

- `vserver cifs group-policy modify`

Learn more

- DOC /protocols/cifs/services

Parameters

Name	Type	In	Required	Description
force	boolean	query	False	If this is set and a machine account with the same name as specified in 'cifs-server name' exists in the Active Directory, existing machine account will be overwritten and reused. The default value for this field is false. • Introduced in: 9.11

Name	Type	In	Required	Description
return_timeout	integer	query	False	The number of seconds to allow the call to execute before returning. When doing a POST, PATCH, or DELETE operation on a single record, the default is 0 seconds. This means that if an asynchronous operation is started, the server immediately returns HTTP code 202 (Accepted) along with a link to the job. If a non-zero value is specified for POST, PATCH, or DELETE operations, ONTAP waits that length of time to see if the job completes so it can return something other than 202. • Default value: 0 • Max value: 120 • Min value: 0
svm.uuid	string	path	True	UUID of the SVM to which this object belongs.

Request Body

Name	Type	Description
ad_domain	ad_domain	
auth-style	string	Authentication type.

Name	Type	Description
auth_user_type	string	Specifies the type of user who can access the SMB Volume. The default is domain_user. In the case of a hybrid-user, ONTAP won't contact on-premise ADDS. • enum: ["domain_user", "hybrid_user"] • Introduced in: 9.16 • x-nullable: true
authentication_method	string	Specifies the authentication method. The available values are: • client_secret • certificate
client_certificate	string	PKCS12 certificate used by the application to prove its identity to AKV.
client_id	string	Application client ID of the deployed Azure application with appropriate access to an AKV or EntraId.
client_secret	string	Secret used by the application to prove its identity to AKV.
comment	string	A descriptive text comment for the CIFS server. SMB clients can see the CIFS server comment when browsing servers on the network. If there is a space in the comment, you must enclose the entire string in quotation marks.
default_unix_user	string	Specifies the UNIX user to which any authenticated CIFS user is mapped to, if the normal user mapping rules fails.
enabled	boolean	Specifies if the CIFS service is administratively enabled.
group_policy_object_enabled	boolean	If set to true, group policies will be applied to the SVM.

Name	Type	Description
key_vault_uri	string	URI of the deployed AKV that is used by ONTAP for storing keys. • example: https://kmip-akv-keyvault.vault.azure.net/ • format: uri • Introduced in: 9.15 • x-nullable: true
name	string	The name of the CIFS server.
netbios	cifs_netbios	
oauth_host	string	Open authorization server host name.
options	cifs_service_options	
proxy_host	string	Proxy host.
proxy_password	string	Proxy password. Password is not audited.
proxy_port	integer	Proxy port.
proxy_type	string	Proxy type.
proxy_username	string	Proxy username.
security	cifs_service_security	
tenant_id	string	Directory (tenant) ID of the deployed Azure application with appropriate access to an AKV or EntraId.
timeout	integer	AKV connection timeout, in seconds. The allowed range is between 0 to 30 seconds.
verify_host	boolean	Verify the identity of the AKV host name. By default, verify_host is set to true.
workgroup	string	The workgroup name.

Example request

```json
{
  "ad_domain": {
    "default_site": "string",
    "fqdn": "example.com",
    "organizational_unit": "string",
    "password": "string",
    "user": "string"
  },
  "auth-style": "domain",
  "auth_user_type": "string",
  "authentication_method": "string",
  "client_certificate": "PEM Cert",
  "client_id": "e959d1b5-5a63-4284-9268-851e30e3eceb",
  "client_secret": "<APPLICATION-CLIENT-SECRET-FOR-AKV>",
  "comment": "This CIFS Server Belongs to CS Department",
  "default_unix_user": "string",
  "key_vault_uri": "https://kmip-akv-keyvault.vault.azure.net/",
  "name": "CIFS1",
  "netbios": {
    "aliases": [
      "ALIAS_1",
      "ALIAS_2",
      "ALIAS_3"
    ],
    "wins_servers": [
      "10.224.65.20",
      "10.224.65.21"
    ]
  },
  "oauth_host": "login.microsoftonline.com",
  "options": {
    "max_connections_per_session": 32,
    "max_lifs_per_session": 256,
    "max_opens_same_file_per_tree": 1000,
    "max_same_tree_connect_per_session": 5000,
    "max_same_user_sessions_per_connection": 2500,
    "max_watches_set_per_tree": 500,
    "null_user_windows_name": "string",
    "smb_credits": 128,
    "widelink_reparse_versions": [
      "smb1"
    ]
  },
  "proxy_host": "proxy.eng.com",
```

```
    "proxy_password": "proxypassword",
    "proxy_port": 1234,
    "proxy_type": "string",
    "proxy_username": "proxyuser",
    "security": {
      "advertised_kdc_encryptions": [
        "string"
      ],
      "lm_compatibility_level": "string",
      "restrict_anonymous": "string",
      "session_security": "string"
    },
    "tenant_id": "c9f32fcb-4ab7-40fe-af1b-1850d46cfbbe",
    "timeout": 25,
    "workgroup": "workgrp1"
  }
```

Response

```
Status: 200, Ok
```

Name	Type	Description
job	job_link	

Example response

```
{
  "job": {
    "uuid": "string"
  }
}
```

Response

```
Status: 202, Accepted
```

Error

```
Status: Default
```

ONTAP Error Response Codes

Error Code	Description
3735751	Failed to authenticate and retrieve the access token from the Azure OAuth host.
3735752	Failed to extract the private key from the Azure Key Vault certificate.
3735753	Unsupported content_type in the Azure secrets response.
3735754	Failed to parse the JSON response from Azure Key Vault.
3735755	REST API call to Azure failed.
3735756	Invalid client certificate.
3735757	Failed to generate client assertion.
3735762	The provided Azure Key Vault configuration is incorrect.
3735763	The provided Azure Key Vault configuration is incomplete.
3735764	Request to Azure failed. Reason - Azure error code and Azure error message.
655390	Failed to modify the CIFS server. Failure can occur due to multiple reasons. For example: STARTTLS and LDAPS cannot be used together or the group policy is already enabled for the SVM.
655562	NetBIOS name is longer than 15 characters.
655538	Unable to modify the CIFS server. The server name is already used by another SVM.
655563	NetBIOS name contains characters that are not allowed.
655771	The number of NetBIOS aliases cannot exceed the maximum supported number of '200'.
655923	Retrieving credentials from AKV is not supported because the effective cluster version is not ONTAP 9.15.0 or later.
656473	Fields security.kdc_encryption and security.advertised_kdc_encryptions are mutually exclusive. Specify only one of the two.

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

ad_domain

Name	Type	Description
default_site	string	The default site used by LIFs that do not have a site membership.
fqdn	string	The fully qualified domain name of the Windows Active Directory to which this CIFS server belongs. A CIFS server appears as a member of Windows server object in the Active Directory store. POST and PATCH only.
organizational_unit	string	Specifies the organizational unit within the Active Directory domain to associate with the CIFS server. POST and PATCH only.
password	string	The account password used to add this CIFS server to the Active Directory. This is not audited.
user	string	The user account used to add this CIFS server to the Active Directory.

iops

The rate of I/O operations observed at the storage object.

Name	Type	Description
other	integer	Performance metric for other I/O operations. Other I/O operations can be metadata operations, such as directory lookups and so on.

Name	Type	Description
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

latency

The round trip latency in microseconds observed at the storage object.

Name	Type	Description
other	integer	Performance metric for other I/O operations. Other I/O operations can be metadata operations, such as directory lookups and so on.
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

throughput

The rate of throughput bytes per second observed at the storage object.

Name	Type	Description
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

metric

Performance numbers, such as IOPS latency and throughput, for SVM protocols.

Name	Type	Description
duration	string	The duration over which this sample is calculated. The time durations are represented in the ISO-8601 standard format. Samples can be calculated over the following durations:
iops	iops	The rate of I/O operations observed at the storage object.
latency	latency	The round trip latency in microseconds observed at the storage object.
status	string	Any errors associated with the sample. For example, if the aggregation of data over multiple nodes fails then any of the partial errors might be returned, "ok" on success, or "error" on any internal uncategorized failure. Whenever a sample collection is missed but done at a later time, it is back filled to the previous 15 second timestamp and tagged with "backfilled_data". "Inconsistent_ delta_time" is encountered when the time between two collections is not the same for all nodes. Therefore, the aggregated value might be over or under inflated. "Negative_delta" is returned when an expected monotonically increasing value has decreased in value. "Inconsistent_old_data" is returned when one or more nodes do not have the latest data.
throughput	throughput	The rate of throughput bytes per second observed at the storage object.
timestamp	string	The timestamp of the performance data.

cifs_netbios

Name	Type	Description
aliases	array[string]	
enabled	boolean	Specifies whether NetBios name service (NBNS) is enabled for the CIFS. If this service is enabled, the CIFS server will start sending the broadcast for name registration.
wins_servers	array[string]	

cifs_service_options

Name	Type	Description
admin_to_root_mapping	boolean	Specifies whether or not Administrator can be mapped to the UNIX user "root".
advanced_sparse_file	boolean	Specifies whether or not the CIFS server supports the advanced sparse file capabilities. This allows CIFS clients to query the allocated ranges of a file and to write zeroes or free data blocks for ranges of a file.
backup_symlink_enabled	boolean	Specifies whether or not to preserve UNIX symlinks during backup through SMB.
client_dup_detection_enabled	boolean	Specifies whether or not client duplicate session detection is enabled for CIFS.
client_version_reporting_enabled	boolean	Specifies whether or not client version reporting is enabled for CIFS.

Name	Type	Description
copy_offload	boolean	Specifies whether or not to enable the Copy Offload feature. This feature enables direct data transfers within or between compatible storage devices without transferring the data through the host computer. Note that this will also enable/disable the direct copy feature accordingly.
dac_enabled	boolean	Specifies whether or not the Dynamic Access Control (DAC) feature is enabled for the CIFS server.
export_policy_enabled	boolean	Specifies whether or not export policies are enabled for CIFS.
fake_open	boolean	Specifies whether or not fake open support is enabled. This parameter allows you to optimize the open and close requests coming from SMB 2 clients.
fsctl_trim	boolean	Specifies whether or not the trim requests (FSCTL_FILE_LEVEL_TRIM) are supported on the CIFS server.
junction_reparse	boolean	Specifies whether or not the reparse point support is enabled. When enabled the CIFS server exposes junction points to Windows clients as reparse points. This parameter is only active if the client has negotiated use of the SMB 2 or SMB 3 protocol. This parameter is not supported for SVMs with Infinite Volume.
large_mtu	boolean	Specifies whether or not SMB clients can send reads up to 1 MB in size.

Name	Type	Description
max_connections_per_session	integer	Specifies the maximum number of connections allowed per multichannel session.
max_lifs_per_session	integer	Specifies the maximum number of LIFs advertised per multichannel session.
max_opens_same_file_per_tree	integer	Specifies the maximum number of opens on the same file per tree.
max_same_tree_connect_per_session	integer	Specifies the maximum number of same tree connections per session.
max_same_user_sessions_per_connection	integer	Specifies the maximum number of same user sessions per connection.
max_watches_set_per_tree	integer	Specifies the maximum number of watches set per tree.
multichannel	boolean	Specifies whether or not the CIFS server supports Multichannel.
null_user_windows_name	string	Specifies a Windows User or Group name that should be mapped in case of a NULL user value.
path_component_cache	boolean	Specifies whether or not the path component cache is enabled on the CIFS server.
referral	boolean	Specifies whether or not to refer clients to more optimal LIFs. When enabled, it automatically refers clients to a data LIF local to the node which hosts the root of the requested share.

Name	Type	Description
shadowcopy	boolean	Specifies whether or not to enable the Shadowcopy Feature. This feature enables to take share-based backup copies of data that is in a data-consistent state at a specific point in time where the data is accessed over SMB 3.0 shares.
shadowcopy_dir_depth	integer	Specifies the maximum level of subdirectories on which ONTAP should create shadow copies. • Default value: 5 • Introduced in: 9.11 • x-nullable: true
smb_credits	integer	Specifies the maximum number of outstanding requests on a CIFS connection.
trusted_domain_enum_search_enabled	boolean	Specifies whether or not to enable trusted domain search. • If this parameter is set to true, it displays CIFS options only for CIFS servers that support enumeration of bidirectional trusted domains and that support searching in all bidirectional trusted domains when performing Windows user lookups for UNIX user to Windows user name mapping. • If set to false, it displays CIFS options for CIFS servers that do not support enumeration of bidirectional trusted domains.
widelink_reparse_versions	array[string]	Specifies the CIFS protocol versions for which the widelink is reported as reparse point.

cifs_service_security

Name	Type	Description
advertised_kdc_encryptions	array[string]	
aes_netlogon_enabled	boolean	Specifies whether or not an AES session key is enabled for the Netlogon channel.
encrypt_dc_connection	boolean	Specifies whether encryption is required for domain controller connections.

Name	Type	Description
kdc_encryption	boolean	(i) This attribute has been deprecated. Use "security.advertised_kdc_encryptions" to specify the encryption type to use. Specifies whether AES-128 and AES-256 encryption is enabled for all Kerberos-based communication with the Active Directory KDC. To take advantage of the strongest security with Kerberos-based communication, AES-256 and AES-128 encryption can be enabled on the CIFS server. Kerberos-related communication for CIFS is used during CIFS server creation on the SVM, as well as during the SMB session setup phase. The CIFS server supports the following encryption types for Kerberos communication:

• RC4-HMAC

• DES

• AES When the CIFS server is created, the domain controller creates a computer machine account in Active Directory. After a newly created machine account authenticates, the KDC and the CIFS server negotiates encryption types. At this time, the KDC becomes aware of the encryption capabilities of the particular machine account and uses those

Name	Type	Description
ldap_referral_enabled	boolean	Specifies whether or not LDAP referral chasing is enabled for AD LDAP connections.
lm_compatibility_level	string	It is CIFS server minimum security level, also known as the LMCompatibilityLevel. The minimum security level is the minimum level of the security tokens that the CIFS server accepts from SMB clients. The available values are: • lm_ntlm_ntlmv2_krb Accepts LM, NTLM, NTLMv2 and Kerberos • ntlm_ntlmv2_krb Accepts NTLM, NTLMv2 and Kerberos • ntlmv2_krb Accepts NTLMv2 and Kerberos • krb Accepts Kerberos only
restrict_anonymous	string	Specifies what level of access an anonymous user is granted. An anonymous user (also known as a "null user") can list or enumerate certain types of system information from Windows hosts on the network, including user names and details, account policies, and share names. Access for the anonymous user can be controlled by specifying one of three access restriction settings. The available values are: • no_restriction - No access restriction for an anonymous user. • no_enumeration - Enumeration is restricted for an anonymous user. • no_access - All access is restricted for an anonymous user.

Name	Type	Description
session_security	string	Specifies client session security for AD LDAP connections. The available values are: • none - No Signing or Sealing. • sign - Sign LDAP traffic. • seal - Seal and Sign LDAP traffic
smb_encryption	boolean	Specifies whether encryption is required for incoming CIFS traffic.
smb_signing	boolean	Specifies whether signing is required for incoming CIFS traffic. SMB signing helps to ensure that network traffic between the CIFS server and the client is not compromised.
try_ldap_channel_binding	boolean	Specifies whether or not channel binding is attempted in the case of TLS/LDAPS.
use_ldaps	boolean	Specifies whether or not to use use LDAPS for secure Active Directory LDAP connections by using the TLS/SSL protocols.
use_start_tls	boolean	Specifies whether or not to use SSL/TLS for allowing secure LDAP communication with Active Directory LDAP servers.

iops_raw

The number of I/O operations observed at the storage object. This should be used along with delta time to calculate the rate of I/O operations per unit of time.

Name	Type	Description
other	integer	Performance metric for other I/O operations. Other I/O operations can be metadata operations, such as directory lookups and so on.

Name	Type	Description
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

latency_raw

The raw latency in microseconds observed at the storage object. This should be divided by the raw IOPS value to calculate the average latency per I/O operation.

Name	Type	Description
other	integer	Performance metric for other I/O operations. Other I/O operations can be metadata operations, such as directory lookups and so on.
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

throughput_raw

Throughput bytes observed at the storage object. This should be used along with delta time to calculate the rate of throughput bytes per unit of time.

Name	Type	Description
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

statistics

These are raw performance numbers, such as IOPS latency and throughput for SVM protocols. These numbers are aggregated across all nodes in the cluster and increase with the uptime of the cluster.

Name	Type	Description
iops_raw	iops_raw	The number of I/O operations observed at the storage object. This should be used along with delta time to calculate the rate of I/O operations per unit of time.
latency_raw	latency_raw	The raw latency in microseconds observed at the storage object. This should be divided by the raw IOPS value to calculate the average latency per I/O operation.
status	string	Any errors associated with the sample. For example, if the aggregation of data over multiple nodes fails then any of the partial errors might be returned, "ok" on success, or "error" on any internal uncategorized failure. Whenever a sample collection is missed but done at a later time, it is back filled to the previous 15 second timestamp and tagged with "backfilled_data". "Inconsistent_delta_time" is encountered when the time between two collections is not the same for all nodes. Therefore, the aggregated value might be over or under inflated. "Negative_delta" is returned when an expected monotonically increasing value has decreased in value. "Inconsistent_old_data" is returned when one or more nodes do not have the latest data.
throughput_raw	throughput_raw	Throughput bytes observed at the storage object. This should be used along with delta time to calculate the rate of throughput bytes per unit of time.

Name	Type	Description
timestamp	string	The timestamp of the performance data.

svm

SVM, applies only to SVM-scoped objects.

Name	Type	Description
name	string	The name of the SVM. This field cannot be specified in a PATCH method.
uuid	string	The unique identifier of the SVM. This field cannot be specified in a PATCH method.

cifs_service

Name	Type	Description
ad_domain	ad_domain	
auth-style	string	Authentication type.
auth_user_type	string	Specifies the type of user who can access the SMB Volume. The default is domain_user. In the case of a hybrid-user, ONTAP won't contact on-premise ADDS. • enum: ["domain_user", "hybrid_user"] • Introduced in: 9.16 • x-nullable: true
authentication_method	string	Specifies the authentication method. The available values are: • client_secret • certificate
client_certificate	string	PKCS12 certificate used by the application to prove its identity to AKV.

Name	Type	Description
client_id	string	Application client ID of the deployed Azure application with appropriate access to an AKV or EntraId.
client_secret	string	Secret used by the application to prove its identity to AKV.
comment	string	A descriptive text comment for the CIFS server. SMB clients can see the CIFS server comment when browsing servers on the network. If there is a space in the comment, you must enclose the entire string in quotation marks.
default_unix_user	string	Specifies the UNIX user to which any authenticated CIFS user is mapped to, if the normal user mapping rules fails.
enabled	boolean	Specifies if the CIFS service is administratively enabled.
group_policy_object_enabled	boolean	If set to true, group policies will be applied to the SVM.
key_vault_uri	string	URI of the deployed AKV that is used by ONTAP for storing keys. • example: https://kmip-akv-keyvault.vault.azure.net/ • format: uri • Introduced in: 9.15 • x-nullable: true
name	string	The name of the CIFS server.
netbios	cifs_netbios	
oauth_host	string	Open authorization server host name.
options	cifs_service_options	
proxy_host	string	Proxy host.

Name	Type	Description
proxy_password	string	Proxy password. Password is not audited.
proxy_port	integer	Proxy port.
proxy_type	string	Proxy type.
proxy_username	string	Proxy username.
security	cifs_service_security	
tenant_id	string	Directory (tenant) ID of the deployed Azure application with appropriate access to an AKV or EntraId.
timeout	integer	AKV connection timeout, in seconds. The allowed range is between 0 to 30 seconds.
verify_host	boolean	Verify the identity of the AKV host name. By default, verify_host is set to true.
workgroup	string	The workgroup name.

job_link

Name	Type	Description
uuid	string	The UUID of the asynchronous job that is triggered by a POST, PATCH, or DELETE operation.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

Retrieve CIFS protocol historical performance metrics for an SVM

GET `/protocols/cifs/services/{svm.uuid}/metrics`

Introduced In: 9.7

Retrieves historical performance metrics for the CIFS protocol of an SVM.

Parameters

Name	Type	In	Required	Description
duration	string	query	False	Filter by duration
status	string	query	False	Filter by status
latency.other	integer	query	False	Filter by latency.other
latency.total	integer	query	False	Filter by latency.total
latency.write	integer	query	False	Filter by latency.write
latency.read	integer	query	False	Filter by latency.read
iops.other	integer	query	False	Filter by iops.other
iops.total	integer	query	False	Filter by iops.total
iops.write	integer	query	False	Filter by iops.write
iops.read	integer	query	False	Filter by iops.read

Name	Type	In	Required	Description
throughput.other	integer	query	False	Filter by throughput.other
throughput.total	integer	query	False	Filter by throughput.total
throughput.write	integer	query	False	Filter by throughput.write
throughput.read	integer	query	False	Filter by throughput.read
timestamp	string	query	False	Filter by timestamp
svm.uuid	string	path	True	Unique identifier of the SVM.

Name	Type	In	Required	Description
interval	string	query	False	The time range for the data. Examples can be 1h, 1d, 1m, 1w, 1y. The period for each time range is as follows:
				• 1h: Metrics over the most recent hour sampled over 15 seconds.
				• 1d: Metrics over the most recent day sampled over 5 minutes.
				• 1w: Metrics over the most recent week sampled over 30 minutes.
				• 1m: Metrics over the most recent month sampled over 2 hours.
				• 1y: Metrics over the most recent year sampled over a day.
				• Default value: 1
				• enum: ["1h", "1d", "1w", "1m", "1y"]

Name	Type	In	Required	Description
return_timeout	integer	query	False	The number of seconds to allow the call to execute before returning. When iterating over a collection, the default is 15 seconds. ONTAP returns earlier if either max records or the end of the collection is reached. • Default value: 15 • Max value: 120 • Min value: 0
fields	array[string]	query	False	Specify the fields to return.
max_records	integer	query	False	Limit the number of records returned.
order_by	array[string]	query	False	Order results by specified fields and optional [asc
desc] direction. Default direction is 'asc' for ascending.	return_records	boolean	query	False

Response

```
Status: 200, Ok
```

Name	Type	Description
_links	_links	
num_records	integer	Number of records
records	array[records]	

Example response

```json
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": [
    {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "duration": "PT15S",
      "iops": {
        "read": 200,
        "total": 1000,
        "write": 100
      },
      "latency": {
        "read": 200,
        "total": 1000,
        "write": 100
      },
      "status": "ok",
      "throughput": {
        "read": 200,
        "total": 1000,
        "write": 100
      },
      "timestamp": "2017-01-25 11:20:13 +0000"
    }
  ]
}
```

Error

```
Status: Default, Error
```

Name	Type	Description
error	returned_error	

Example error

```
{
  "error": {
    "arguments": [
      {
        "code": "string",
        "message": "string"
      }
    ],
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```

Definitions

See Definitions

href

Name	Type	Description
href	string	

_links

Name	Type	Description
next	href	
self	href	

_links

Name	Type	Description
self	href	

iops

The rate of I/O operations observed at the storage object.

Name	Type	Description
other	integer	Performance metric for other I/O operations. Other I/O operations can be metadata operations, such as directory lookups and so on.
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

latency

The round trip latency in microseconds observed at the storage object.

Name	Type	Description
other	integer	Performance metric for other I/O operations. Other I/O operations can be metadata operations, such as directory lookups and so on.
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

throughput

The rate of throughput bytes per second observed at the storage object.

Name	Type	Description
other	integer	Performance metric for other I/O operations. Other I/O operations can be metadata operations, such as directory lookups and so on.
read	integer	Performance metric for read I/O operations.
total	integer	Performance metric aggregated over all types of I/O operations.
write	integer	Performance metric for write I/O operations.

records

Performance numbers, such as IOPS latency and throughput.

Name	Type	Description
_links	_links	

Name	Type	Description
duration	string	The duration over which this sample is calculated. The time durations are represented in the ISO-8601 standard format. Samples can be calculated over the following durations:
iops	iops	The rate of I/O operations observed at the storage object.
latency	latency	The round trip latency in microseconds observed at the storage object.
status	string	Errors associated with the sample. For example, if the aggregation of data over multiple nodes fails, then any partial errors might return "ok" on success or "error" on an internal uncategorized failure. Whenever a sample collection is missed but done at a later time, it is back filled to the previous 15 second timestamp and tagged with "backfilled_data". "Inconsistent_delta_time" is encountered when the time between two collections is not the same for all nodes. Therefore, the aggregated value might be over or under inflated. "Negative_delta" is returned when an expected monotonically increasing value has decreased in value. "Inconsistent_old_data" is returned when one or more nodes do not have the latest data.
throughput	throughput	The rate of throughput bytes per second observed at the storage object.
timestamp	string	The timestamp of the performance data.

error_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

returned_error

Name	Type	Description
arguments	array[error_arguments]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.