oVirt SSO Specification

Behavior Changes

End user visible changes

The password delegation checkbox at user portal login is now a profile setting.

Sysadmin visible changes

Apache negotiation URL change

Kerberos or any other negotiation module should not be applied to entire URI namespace, this provide huge performance improvement and greater flexibility.
See Misc section of apache configuration example.

RestAPI visible changes

RestAPI negotiation authentication

RestAPI negotiation authentication is disabled by default, application should use the new OAuth2 interface in order to acquire a token.
This can be re-enabled by engine configuration ENGINE_RESTAPI_NEGO and adding |^/ovirt-engine/api to LocationMatch of apache configuration.
Notice: in most cases this will have negative performance impact due to HTTP renegotiation.

OAuth2

Outline

The oVirt SSO service is OAuth2 compliant with minimal features.

References

http://tools.ietf.org/html/rfc6749
http://tools.ietf.org/html/rfc6750
https://tools.ietf.org/html/draft-ietf-oauth-introspection-04
https://developer.github.com/v3/oauth/
https://aaronparecki.com/articles/2012/07/29/1/oauth2-simplified
https://developer.linkedin.com/docs/oauth2

/sso/oauth/authorize

Query String Parameters

Name	Type	Description
client_id	string	Required: Client unique id, provided at registration time.
response_type	string	"code"
scope	string	A space delimited list of scopes. If not provided a default will be used.
redirect_uri	string	The URL to which to redirect after authorization. It must

		match the base URL that was provided at registration time.
state	string	Cross site protection, sent as a parameter to the redirection_uri.

redirection_uri query String Parameters

Name	Type	Description
state	string	The content of state sent to authorize.
code	string	The authorization code. Base64 alphabet long string.

Error codes

Name	Description
invalid_request	The request is missing a required parameter, includes an unsupported parameter value.
unauthorized_client	The client is not authorized to request an authorization code using this method.
access_denied	The resource owner or authorization server denied the request.
invalid_scope	The requested scope is invalid, unknown, malformed, or exceeds the scope granted by the resource owner.
server_error	Any other server error.
temporarily_unavailable	...
ovirt_not_authenticated	if not logged in.

/sso/oauth/token[authorization_code]

Headers

Name	Type	Description
Authorization	string	Basic authorization header of client_id as a user and client_secret as a password.
ContentType	String	application/x-www-form-urlencoded
Accept	string	Response form. Supported: application/json

POST parameters

Name	Type	Description

client_id	string	Required: Client unique id, provided at registration time. [fallback to authorization header].
client_secret	string	Required: Client secret, provided at registration time. [fallback to authorization header].
grant_type	string	"authorization_code"
code	string	Required: The authorization code. Base64 alphabet long string.
redirect_uri	string	Must be valid for client_id but not actually used(?!?).

Response

application/json

```
{
        "access_token": "token",
        "scope": "space_delimited_scopes",
        "expires_in": "lifetime_in_seconds", # taken out of auth record
        "token_type": "bearer"
}
```

Error codes

Name	**Description**
invalid_request	The request is missing a required parameter, includes an unsupported parameter value.
unauthorized_client	The client is not authorized to request an authorization code using this method.
access_denied	The resource owner or authorization server denied the request.
invalid_grant	The provided authorization grant (e.g., authorization code, resource owner credentials) or refresh token is invalid, expired, revoked, does not match the redirection URI used in the authorization request, or was issued to another client.
unsupported_response_type	The authorization server does not support obtaining an access token using this method.
invalid_scope	The requested scope is invalid, unknown, malformed, or exceeds the scope granted by the resource owner.
server_error	Any other server error.
temporarily_unavailable	...

/sso/oauth/token[password]

Headers

Name	Type	Description
Authorization	string	Authorization headers for client.
ContentType	String	application/x-www-form-urlencoded
Accept	string	Response form. Supported: application/json

POST parameters

Name	Type	Description
client_id	string	Required: Client unique id, provided at registration time. [fallback to authorization header].
client_secret	string	Required: Client secret, provided at registration time. [fallback to authorization header].
grant_type	string	"password"
username	string	Required: User name.
password	string	Required: User's Password.
scope	string	A space delimited list of scopes. If not provided a default will be used.
ovirt_auth_record	string	Optional: ovirt proprietary auto record applicable when login on behalf is used.

Response

application/json

```
{
        "access_token": "token",
        "scope": "space_delimited_scopes",
        "expires_in": "lifetime_in_seconds", # taken out of auth record
        "token_type": "bearer"
}
```

Error codes

Name	Description
invalid_request	The request is missing a required parameter, includes an unsupported parameter value.
unauthorized_client	The client is not authorized to request an authorization

	code using this method.
access_denied	The resource owner or authorization server denied the request.
invalid_grant	The provided authorization grant (e.g., authorization code, resource owner credentials) or refresh token is invalid, expired, revoked, does not match the redirection URI used in the authorization request, or was issued to another client.
unsupported_grant_type	The authorization grant type is not supported by the authorization server.
invalid_scope	The requested scope is invalid, unknown, malformed, or exceeds the scope granted by the resource owner.
server_error	Any other server error.
temporarily_unavailable	...

/sso/oauth/token[-http-auth][urn:ovirt:params:oauth:grant-type:http]

This is an extension to OAuth2 to enable authenticating a user (Resource Owner) with standard HTTP authorization headers. This will enable SPENGO or other methods to be usable while are not usable in the password grant_type.

Headers

Name	Type	Description
Authorization	string	Authorization headers for user.
ContentType	String	application/x-www-form-urlencoded
Accept	string	Response form. Supported: application/json

Query and/or POST parameters

Name	Type	Description
grant_type	string	"urn:ovirt:params:oauth:grant-type:http"
scope	string	A space delimited list of scopes. If not provided a default will be used.

Response

application/json

```
{
        "access_token": "token",
        "scope": "space_delimited_scopes",
        "expires_in": "lifetime_in_seconds", # taken out of auth record
```

```
    "token_type": "bearer"
}
```

Error codes

Name	Description
invalid_request	The request is missing a required parameter, includes an unsupported parameter value.
access_denied	The resource owner or authorization server denied the request.
unsupported_grant_type	The authorization grant type is not supported by the authorization server.
invalid_scope	The requested scope is invalid, unknown, malformed, or exceeds the scope granted by the resource owner.
server_error	Any other server error.
temporarily_unavailable	...

/sso/oauth/token_info

Headers

Name	Type	Description
Authorization	string	Basic authorization header of client_id as a user and client_secret as a password.
ContentType	string	application/x-www-form-urlencoded
Accept	string	Response form. Supported: application/json

POST parameters

Name	Type	Description
client_id	string	Required: Client unique id, provided at registration time. [fallback to authorization header].
client_secret	string	Required: Client secret, provided at registration time. [fallback to authorization header].
token	string	Required: The access token.
scope	string	A space delimited list of scopes. If not provided a default will be used. Specifying ovirt-auth-validate scope will supress token information in response.

Response

application/json

```
{
        "active": true/false,
        "token_type": "bearer",
        "client_id": "client_id_who_issue_token",
        "user_id": "xx",
        "scope": "space_delimited_scopes",
        "exp": "in_seconds",
        "ovirt": {
                "version": 0,
                "principal_id": external id of the user,
                "email": email address,
                "group_ids": group ids of the user,
                "password": "users' password if ovirt-auth-password-access scope"
        }
}
```

Error codes

Name	Description
invalid_request	The request is missing a required parameter, includes an unsupported parameter value.
unauthorized_client	The client is not authorized to request an authorization code using this method.
invalid_grant	The provided authorization grant (e.g., authorization code, resource owner credentials) or refresh token is invalid, expired, revoked, does not match the redirection URI used in the authorization request, or was issued to another client.
server_error	Any other server error.
temporarily_unavailable	...

/sso/oauth/revoke

oVirt extension to the OAuth2 interface to revoke an access token.
Revoking authentication token can be done without client_id/client_secret credentials, unless special scope is required.

Headers

Name	Type	Description
Authorization	string	Basic authorization header of client_id as a user and client_secret as a password. Or Bearer authentication based on authorization token.

ContentType	string	application/x-www-form-urlencoded
Accept	string	Response form. Supported: application/json

POST parameters

Name	Type	Description
client_id	string	Client unique id, provided at registration time. [fallback to authorization header (Basic)].
client_secret	string	Client secret, provided at registration time. [fallback to authorization header (Basic)].
token	string	Required: The access token. [fallback to authorization header (Bearer)]
scope	string	A space delimited list of scopes. If not provided a default will be used.

Response

application/json

```
{
}
```

Error codes

Name	Description
invalid_request	The request is missing a required parameter, includes an unsupported parameter value.
unauthorized_client	The client is not authorized to request an authorization code using this method.
invalid_grant	The provided authorization grant (e.g., authorization code, resource owner credentials) or refresh token is invalid, expired, revoked, does not match the redirection URI used in the authorization request, or was issued to another client.
invalid_scope	The requested scope is invalid, unknown, malformed, or exceeds the scope granted by the resource owner.
server_error	Any other server error.
temporarily_unavailable	...

Error Response

Response

May be in query string, or json payload.

Name	Description
error	A single ASCII error code.
error_description	Human readable error.
error_uri	A URI of human readable page.

Error codes

Name	Description
invalid_request	The request is missing a required parameter, includes an unsupported parameter value.
invalid_client	Client authentication failed.
invalid_grant	The provided authorization grant is invalid.
invalid_scope	The requested scope is invalid, unknown, malformed, or exceeds the scope granted by the resource owner.

Notification callback

Issued if registered for client.

Headers

Name	Type	Description
ContentType	string	application/x-www-form-urlencoded

POST parameters

Name	Type	Description
event	string	event name: logout
token	string	The token.
token_type	string	bearer

Error codes

None.

Client Application

Accessing application is done by setting the following authorization header:
Authorization: Bearer <token>

Configuration

SSO Configuration

Name	Type	Default	Description
SSO_TOKEN_TIMEOUT	Int	360000	Maximum lifetime in seconds of a token. Was: vdc_options::UserSessionHardLimit
SSO_HOUSE_KEEPING_INTERVAL	Int	60	Interval in which housekeeping occur in seconds.
SSO_AUTH_LOGIN_SEQUENCE	Str	NI	Login sequence to use. B - Basic enforce. b - Basic accept. N - Negotiate. I - Internal.
SSO_TOKEN_HTTP_LOGIN_SEQUENCE	Str	Nb	b - Basic accept. N - Negotiate.
SSO_CALLBACK_PREFIX_CHECK	Bool	true	Enforce OAuth2 callback prefix. Should not be modified.
SSO_PKI_TRUST_STORE	File	"${ENGINE_PKI_TRUST*}"	Trust store for outgoing communications.
SSO_PKI_TRUST_STORE_TYPE	Str	"${ENGINE_PKI_TRUST*}"	Trust store for outgoing communications.
SSO_PKI_TRUST_STORE_PASSWORD	Str	"${ENGINE_PKI_TRUST*}"	Trust store for outgoing communications.
SSO_ENGINE_URL	Str	"http://${ENGINE_FQDN}${ENGINE_URI}"	The engine URL for oVirt logo in login page.

Engine Configuration

Name	Type	Default	Description
ENGINE_SSO_AUTH_URL	Str		SSO URL visible for user agent.
ENGINE_SSO_SERVICE_URL	Str	"${ENGINE_SSO_AUTH_URL}"	SSO service URL for direct communications.
ENGINE_SSO_SERVICE_SSL_PROT	Str	TLSv1	SSL protocol to use.

OCOL			
ENGINE_SSO_SERVICE_SSL_VERIFY_HOST	Bool	True	Enable host verification.
ENGINE_SSO_SERVICE_SSL_VERIFY_CHAIN	Bool	True	Enable chain verification
ENGINE_RESTAPI_NEGO	Bool	False	Enable restapi nego using direct access.
ENGINE_SSO_CLIENT_ID	Str		Client id to use.
ENGINE_SSO_CLIENT_SECRET	Str		Client password to use.
ENGINE_SSO_AUTH_SEQUENCE_app=seq	Str	~	Override auth sequence for this app. app can be: webadmin, userportal, welcome.
ENGINE_ERROR_PAGE	Str	${ENGINE_URI}/error.html	The error page to display when apps receive errors from SSO.

Data Model

SSO Client registration

Persistent, accessible only to SSO service.
Probably in database table.

Name	Type	Description
id	seq	
client_id	string	Unique string, probably uuid.
client_secret	string	PBEEnvelope format
callback_prefix	string	A url prefix for cross site prevention.
certificate_location	string	Optional location of certificate to encrypt password to.
notification_callback	string	Optional location of callback for this client.
notification_callback_protocol	string	SSL protocol to use, default: "TLSv1"
notification_callback_verify_host	boolean	Verify host name when communicating to callback.
notification_callback_verify_chain	boolean	Verify chain when communicating to callback.

description	string	Client description, not actually used.
email	string	Client contact.
scope	string	Space delimited scopes approved for this client.
trusted	boolean	If trusted no user approval dialog will be presented before authentication. **We support only trusted for now.**

SSO token registry

Non persistent storage.

Name	Type	Description
token	string	[Key] access token. base64(random[64bytes])
client_id	string/null	client who issued token.
active	boolean	may hold inactive for a while until cleanup.
code	string/null	authorization code. base64(random[64bytes])
userid	string	unique user id authz:user or similar.
user	string	user name.
validto	timestamp	
scope	string	space delimited scopes
ovirt_auth_record	complex	key: "name;type;uuid" value: json serialize
ovirt_principal_record	complex	
password	string	if ovirt-password-access scope had been requested.

Application SSO credentials

Within engine config, generated by setup.

For now we can have single client_id for all engine applications (api, userportal, webadmin).

Scopes

Global Scopes

Name	Description
ovirt-app-portal	Permit login into user portal.

ovirt-app-admin	Permit login into webadmin.
ovirt-app-api	Permit interaction with API.
ovirt-ext=ext	Ovirt extension, may appear multiple times.

Scope Dependencies

Name	Scopes	Description
ovirt-app-admin ovirt-app-portal	ovirt-app-api ovirt-ext=token:password-access ovirt-ext=token-info:validate ovirt-ext=token:login-on-behalf ovirt-ext=revoke:revoke-all	Internal engine
ovirt-app-api	ovirt-ext=token-info:validate	A restapi client

Auth Extensions

Name	Description
auth:identity	Return existing identity, do not present login form. Callback error code is ovirt_not_authenticated if not authenticated.
token:password-access	Enables user's raw password access. This should not be used in new clients.
token-info:validate	Only perform session validation, does not return data.
auth:sequence-priority=seq	Request to modify login sequence. Available sequences: B - Basic enforce. b - basic accept. I - internal. N - negotiate. sso setting is intersected with the seq settings, if empty result, an error should be presented. if seq begins with ~ then it is prepend to sso setting, removing duplicates before intersecting, this used to set priority to specific method. For example: sso: bNI seq: ~I prepend: IbNI Dup remove: IbN

	intersect: IbN

Token Extensions

Name	Description
token:login-on-behalf	Valid only when grant_type=password, enable login without password check. Care should be taken when assigning this scope to a client.
token:password-access	Enables user's raw password access. This should not be used in new clients.

Token Info Extensions

Name	Description
token-info:validate	Only perform session validation, does not return data.

Revoke Extensions

Name	Description
revoke:revoke-all	Revoke all access tokens of a user. Should be used by authorized application to logout a user completely.

Misc

External Authentication Apache Configuration

```
<LocationMatch ^/ovirt-engine/sso/(interactive-login-negotiate|oauth/token-http-auth)>
        RewriteEngine on
        RewriteCond %{LA-U:REMOTE_USER} ^(.*)$
        RewriteRule ^(.*)$ - [L,P,E=REMOTE_USER:%1]
        RequestHeader set X-Remote-User %{REMOTE_USER}s

        AuthType Kerberos
        AuthName "Kerberos Login"
        Krb5Keytab /etc/krb5.keytab
        KrbAuthRealms REALM
        KrbMethodK5Passwd off
        Require valid-user

        ErrorDocument 401 "<html><meta http-equiv=\"refresh\" content=\"0;
url=/ovirt-engine/sso/login-unauthorized\"/><body><a href=\"/ovirt-engine/sso/
login-unauthorized\">Here</a></body></html>"
</LocationMatch>
```

If ENGINE_RESTAPI_NEGO is enabled, add the following:

```
<LocationMatch ^/ovirt-engine/api>
        RewriteEngine on
        RewriteCond %{LA-U:REMOTE_USER} ^(.*)$
        RewriteRule ^(.*)$ - [L,P,E=REMOTE_USER:%1]
```

```
        RequestHeader set X-Remote-User %{REMOTE_USER}s

        AuthType Kerberos
        AuthName "Kerberos Login"
        Krb5Keytab /etc/krb5.keytab
        KrbAuthRealms REALM
        KrbMethodK5Passwd off
        Require valid-user
</LocationMatch>
```

Examples

RestAPI access

Acquire ticket

HTTP Authentication (Basic)

$ curl -v -k -H "Accept: application/json" 'https://USER:PASSWORD@ENGINE/ovirt-engine/sso/oauth/token?grant_type=urn:ovirt:params:oauth:grant-type:http&scope=ovirt-app-api'

HTTP Authentication (SPNEGO)

$ curl --negotiate --user : -v -k -H "Accept: application/json" 'https://ENGINE/ovirt-engine/sso/oauth/token-http-auth?grant_type=urn:ovirt:params:oauth:grant-type:http&scope=ovirt-app-api'

User/password Authentication

$ curl -v -k -H "Accept: application/json" 'https://ENGINE/ovirt-engine/sso/oauth/token?grant_type=password&username=USER&password=PASSWORD&scope=ovirt-app-api'

Reply

{"access_token":"mWIwC8zJOmLoysbiPEDyLIhUMm1IV9ltW2osSMfh85hJ9nmY-Gph_aalD4FqjTMRQYSwjFuiqIWqDJwD-2dYVQ","scope":"ovirt-app-api ovirt-ext=token-info:validate","exp":2147483647,"token_type":"bearer"}

Access

$ curl -v -k -H "Authorization: Bearer mWIwC8zJOmLoysbiPEDyLIhUMm1IV9ltW2osSMfh85hJ9nmY-Gph_aalD4FqjTMRQYSwjFuiqIWqDJwD-2dYVQ" -L https://engine/ovirt-engine/api