# FIIF 3.11.2022
# OPC UA – Access rights & permissions
# Application level security

Mika Karaila - Valmet

# OPC UA - Security

- Protocol level security is explained multiple times
- Based on username & password, messages crypted with certificates

- Application level security / protection can be done with:
  - Access rights
  - Permissions: role based access
    https://reference.opcfoundation.org/Core/Part2/4.12/

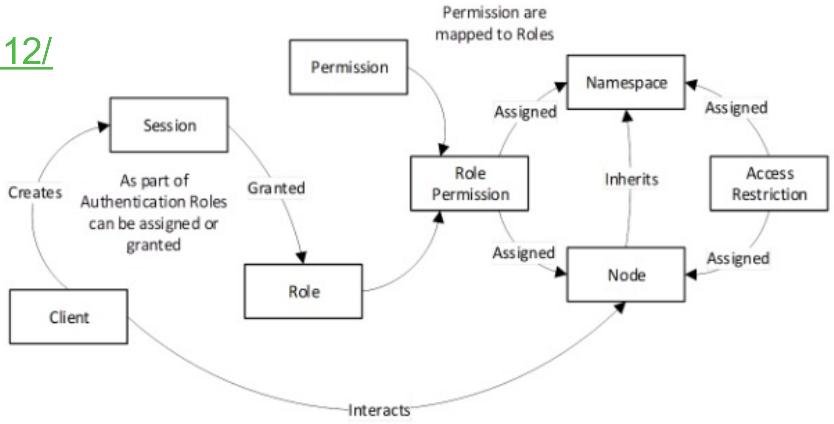


**Figure 4 - Role overview**

For additional description of roles see in in OPC 10000-5

# OPC UA – Access rights

- Access rights are ”static” variable can have following access rights:
  - CurrentRead
  - CurrentWrite
  - HistoryRead
  - Special: NoSubDataTypes, Nonatomicread, Nonatomicwrite, WriteFullArrayOnly

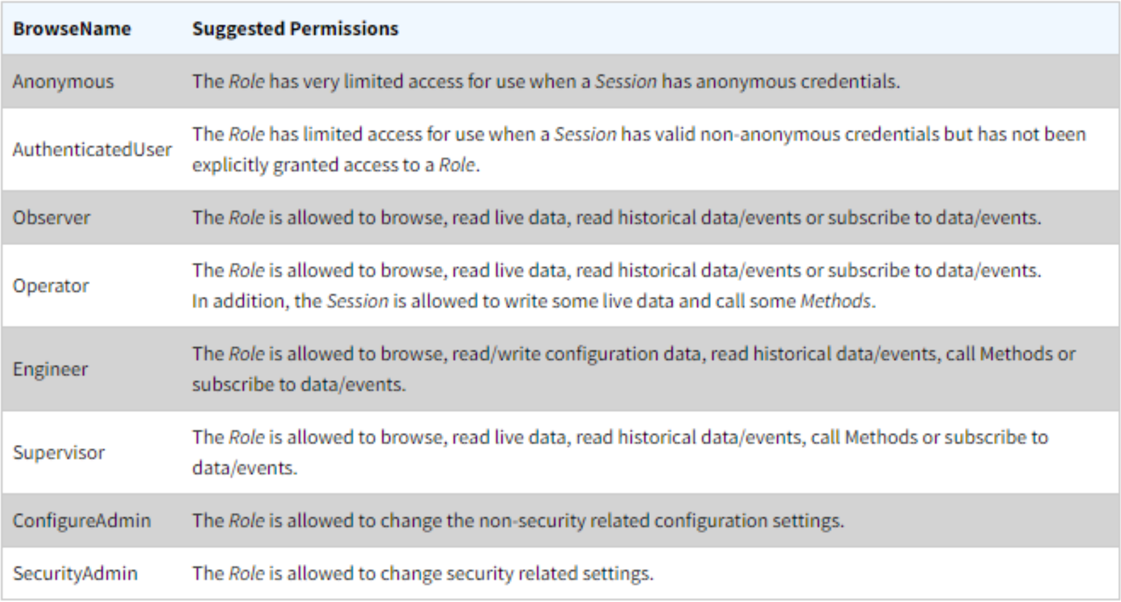
- Normal use cases:
  - Variable can be read / write: ”CurrentRead | CurrentWrite”
  - Read only variable: ”CurrentRead”

# OPC UA – Permissions

## Role based access control (RBAC), username & password + role

- User has given role/roles based on username
- Role(s) selected as user ”logins” => activates session
- WellKnownRoles:
  - Anonymous
  - AuthenticatedUser
  - Observer
  - Operator
  - Engineer
  - Supervisor
  - ConfigureAdmin
  - SecurityAdmin

**Table 2 – Well-Known Roles**

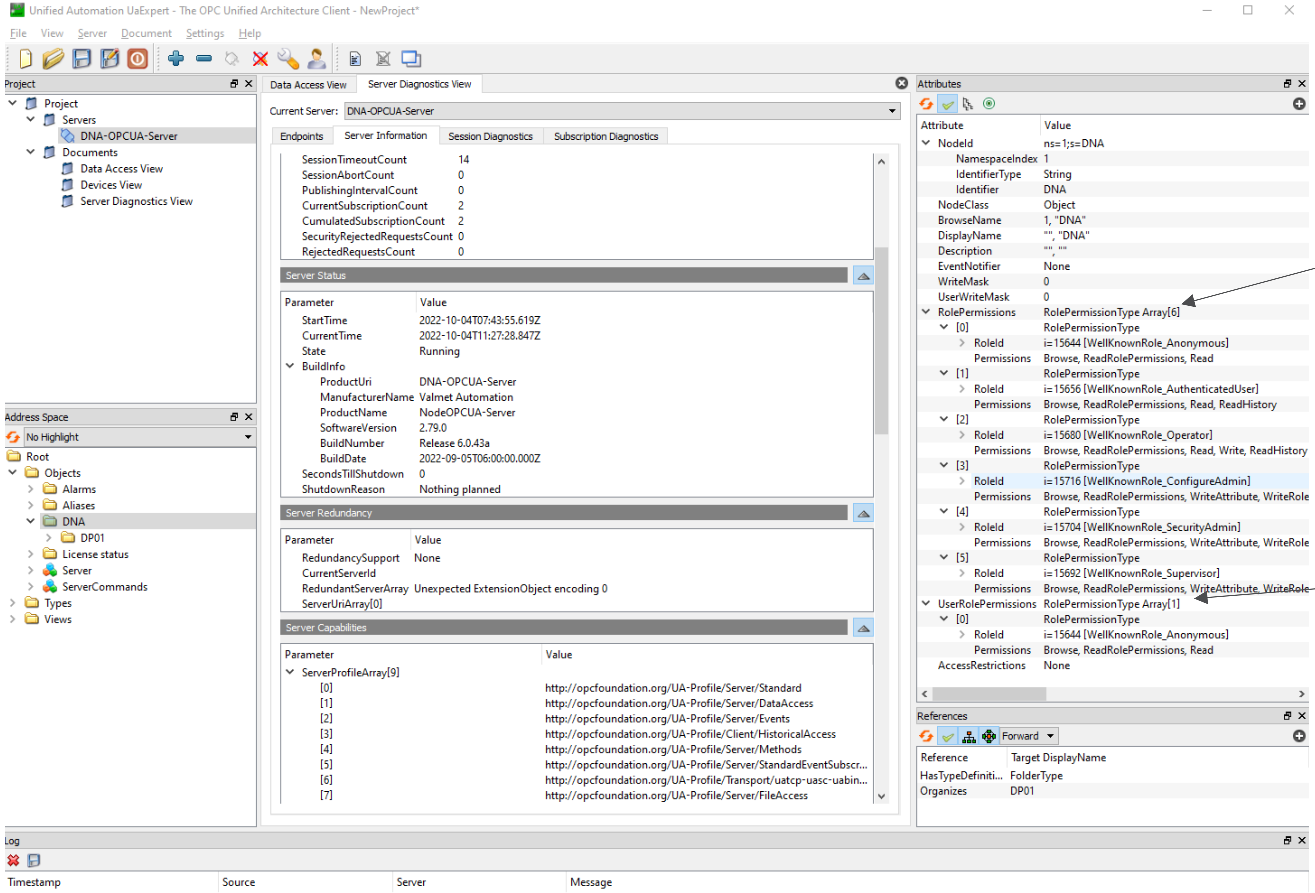


| BrowseName | Suggested Permissions |
|---|---|
| Anonymous | The *Role* has very limited access for use when a *Session* has anonymous credentials. |
| AuthenticatedUser | The *Role* has limited access for use when a *Session* has valid non-anonymous credentials but has not been explicitly granted access to a *Role*. |
| Observer | The *Role* is allowed to browse, read live data, read historical data/events or subscribe to data/events. |
| Operator | The *Role* is allowed to browse, read live data, read historical data/events or subscribe to data/events.<br>In addition, the *Session* is allowed to write some live data and call some *Methods*. |
| Engineer | The *Role* is allowed to browse, read/write configuration data, read historical data/events, call Methods or subscribe to data/events. |
| Supervisor | The *Role* is allowed to browse, read live data, read historical data/events, call Methods or subscribe to data/events. |
| ConfigureAdmin | The *Role* is allowed to change the non-security related configuration settings. |
| SecurityAdmin | The *Role* is allowed to change security related settings. |

https://reference.opcfoundation.org/v104/Core/docs/Part3/4.8.2/

# OPC UA – Testing Access rights & permissions

## UaExpert



Current Server: DNA-OPCUA-Server

| | |
|---|---|
| SessionTimeoutCount | 14 |
| SessionAbortCount | 0 |
| PublishingIntervalCount | 0 |
| CurrentSubscriptionCount | 2 |
| CumulatedSubscriptionCount | 2 |
| SecurityRejectedRequestsCount | 0 |
| RejectedRequestsCount | 0 |

Server Status

| Parameter | Value |
|---|---|
| StartTime | 2022-10-04T07:43:55.619Z |
| CurrentTime | 2022-10-04T11:27:28.847Z |
| State | Running |
| BuildInfo | |
| ProductUri | DNA-OPCUA-Server |
| ManufacturerName | Valmet Automation |
| ProductName | NodeOPCUA-Server |
| SoftwareVersion | 2.79.0 |
| BuildNumber | Release 6.0.43a |
| BuildDate | 2022-09-05T06:00:00.000Z |
| SecondsTillShutdown | 0 |
| ShutdownReason | Nothing planned |

Server Redundancy

| Parameter | Value |
|---|---|
| RedundancySupport | None |
| CurrentServerId | |
| RedundantServerArray | Unexpected ExtensionObject encoding 0 |
| ServerUriArray[0] | |

Server Capabilities

| Parameter | Value |
|---|---|
| ServerProfileArray[9] | |
| [0] | http://opcfoundation.org/UA-Profile/Server/Standard |
| [1] | http://opcfoundation.org/UA-Profile/Server/DataAccess |
| [2] | http://opcfoundation.org/UA-Profile/Server/Events |
| [3] | http://opcfoundation.org/UA-Profile/Client/HistoricalAccess |
| [4] | http://opcfoundation.org/UA-Profile/Server/Methods |
| [5] | http://opcfoundation.org/UA-Profile/Server/StandardEventSubscr... |
| [6] | http://opcfoundation.org/UA-Profile/Transport/uatcp-uasc-uabin... |
| [7] | http://opcfoundation.org/UA-Profile/Server/FileAccess |

| Attribute | Value |
|---|---|
| NodeId | ns=1;s=DNA |
| NamespaceIndex | 1 |
| IdentifierType | String |
| Identifier | DNA |
| NodeClass | Object |
| BrowseName | 1, "DNA" |
| DisplayName | "", "DNA" |
| Description | "", "" |
| EventNotifier | None |
| WriteMask | 0 |
| UserWriteMask | 0 |
| RolePermissions | RolePermissionType Array[6] |
| [0] | RolePermissionType |
| RoleId | i=15644 [WellKnownRole_Anonymous] |
| Permissions | Browse, ReadRolePermissions, Read |
| [1] | RolePermissionType |
| RoleId | i=15656 [WellKnownRole_AuthenticatedUser] |
| Permissions | Browse, ReadRolePermissions, Read, ReadHistory |
| [2] | RolePermissionType |
| RoleId | i=15680 [WellKnownRole_Operator] |
| Permissions | Browse, ReadRolePermissions, Read, Write, ReadHistory |
| [3] | RolePermissionType |
| RoleId | i=15716 [WellKnownRole_ConfigureAdmin] |
| Permissions | Browse, ReadRolePermissions, WriteAttribute, WriteRole |
| [4] | RolePermissionType |
| RoleId | i=15704 [WellKnownRole_SecurityAdmin] |
| Permissions | Browse, ReadRolePermissions, WriteAttribute, WriteRole |
| [5] | RolePermissionType |
| RoleId | i=15692 [WellKnownRole_Supervisor] |
| Permissions | Browse, ReadRolePermissions, WriteAttribute, WriteRole |
| UserRolePermissions | RolePermissionType Array[1] |
| [0] | RolePermissionType |
| RoleId | i=15644 [WellKnownRole_Anonymous] |
| Permissions | Browse, ReadRolePermissions, Read |
| AccessRestrictions | None |

| Reference | Target DisplayName |
|---|---|
| HasTypeDefiniti... | FolderType |
| Organizes | DP01 |

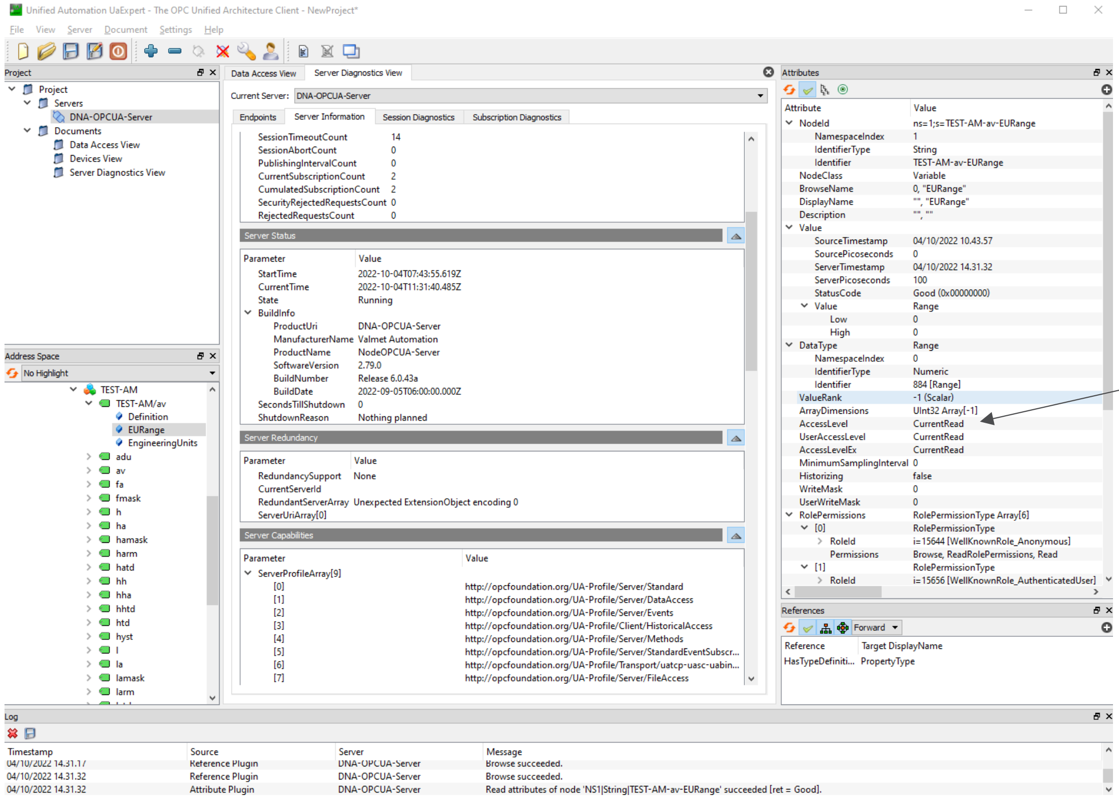
| Timestamp | Source | Server | Message |
|---|---|---|---|

Role permissions

User Role permissions

# OPC UA – Read-only variable: EURange

## UaExpert



Unified Automation UaExpert - The OPC Unified Architecture Client - NewProject*

```
Project
  Project
    Servers
      DNA-OPCUA-Server
    Documents
      Data Access View
      Devices View
      Server Diagnostics View

Address Space
No Highlight
  TEST-AM
    TEST-AM/av
      Definition
      EURange
      EngineeringUnits
    adu
    av
    fa
    fmask
    h
    ha
    hamask
    harm
    hatd
    hh
    hha
    hhtd
    htd
    hyst
    l
    la
    lamask
    larm
```

Current Server: DNA-OPCUA-Server

| | |
|---|---|
| SessionTimeoutCount | 14 |
| SessionAbortCount | 0 |
| PublishingIntervalCount | 0 |
| CurrentSubscriptionCount | 2 |
| CumulatedSubscriptionCount | 2 |
| SecurityRejectedRequestsCount | 0 |
| RejectedRequestsCount | 0 |

Server Status

| Parameter | Value |
|---|---|
| StartTime | 2022-10-04T07:43:55.619Z |
| CurrentTime | 2022-10-04T11:31:40.485Z |
| State | Running |
| BuildInfo | |
| ProductUri | DNA-OPCUA-Server |
| ManufacturerName | Valmet Automation |
| ProductName | NodeOPCUA-Server |
| SoftwareVersion | 2.79.0 |
| BuildNumber | Release 6.0.43a |
| BuildDate | 2022-09-05T06:00:00.000Z |
| SecondsTillShutdown | 0 |
| ShutdownReason | Nothing planned |

Server Redundancy

| Parameter | Value |
|---|---|
| RedundancySupport | None |
| CurrentServerId | |
| RedundantServerArray | Unexpected ExtensionObject encoding 0 |
| ServerUriArray[0] | |

Server Capabilities

| Parameter | Value |
|---|---|
| ServerProfileArray[9] | |
| [0] | http://opcfoundation.org/UA-Profile/Server/Standard |
| [1] | http://opcfoundation.org/UA-Profile/Server/DataAccess |
| [2] | http://opcfoundation.org/UA-Profile/Server/Events |
| [3] | http://opcfoundation.org/UA-Profile/Client/HistoricalAccess |
| [4] | http://opcfoundation.org/UA-Profile/Server/Methods |
| [5] | http://opcfoundation.org/UA-Profile/Server/StandardEventSubscr... |
| [6] | http://opcfoundation.org/UA-Profile/Transport/uatcp-uasc-uabin... |
| [7] | http://opcfoundation.org/UA-Profile/Server/FileAccess |

Attributes

| Attribute | Value |
|---|---|
| NodeId | ns=1;s=TEST-AM-av-EURange |
| NamespaceIndex | 1 |
| IdentifierType | String |
| Identifier | TEST-AM-av-EURange |
| NodeClass | Variable |
| BrowseName | 0, "EURange" |
| DisplayName | "", "EURange" |
| Description | "", "" |
| Value | |
| SourceTimestamp | 04/10/2022 10.43.57 |
| SourcePicoseconds | 0 |
| ServerTimestamp | 04/10/2022 14.31.32 |
| ServerPicoseconds | 100 |
| StatusCode | Good (0x00000000) |
| Value | Range |
| Low | 0 |
| High | 0 |
| DataType | Range |
| NamespaceIndex | 0 |
| IdentifierType | Numeric |
| Identifier | 884 [Range] |
| ValueRank | -1 (Scalar) |
| ArrayDimensions | UInt32 Array[-1] |
| AccessLevel | CurrentRead |
| UserAccessLevel | CurrentRead |
| AccessLevelEx | CurrentRead |
| MinimumSamplingInterval | 0 |
| Historizing | false |
| WriteMask | 0 |
| UserWriteMask | 0 |
| RolePermissions | RolePermissionType Array[6] |
| [0] | RolePermissionType |
| RoleId | i=15644 [WellKnownRole_Anonymous] |
| Permissions | Browse, ReadRolePermissions, Read |
| [1] | RolePermissionType |
| RoleId | i=15656 [WellKnownRole_AuthenticatedUser] |

References

| Reference | Target DisplayName |
|---|---|
| HasTypeDefiniti... | PropertyType |

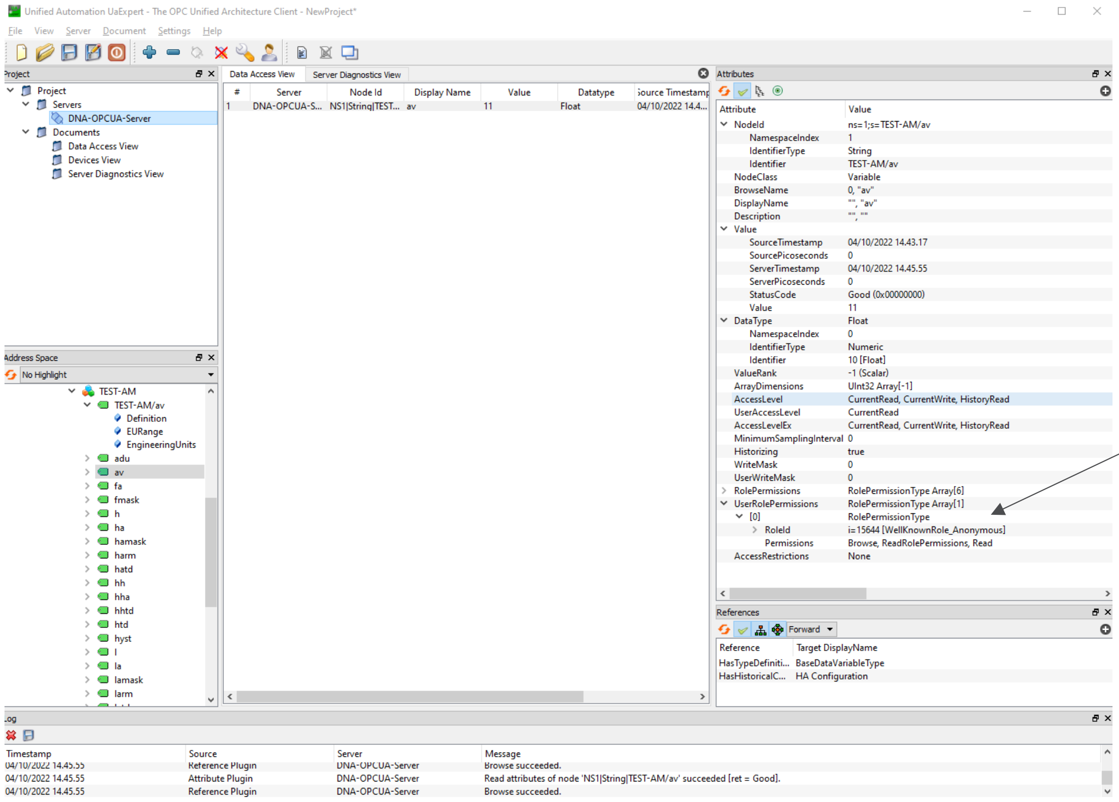
Log

```
Timestamp            Source            Server            Message
04/10/2022 14.31.17  Reference Plugin  DNA-OPCUA-Server  Browse succeeded.
04/10/2022 14.31.32  Reference Plugin  DNA-OPCUA-Server  Browse succeeded.
04/10/2022 14.31.32  Attribute Plugin  DNA-OPCUA-Server  Read attributes of node 'NS1|String|TEST-AM-av-EURange' succeeded [ret = Good].
```

Access rights: CurrentRead

# OPC UA – Anonymous: read-only permissions – no history read!

## UaExpert



| # | Server | Node Id | Display Name | Value | Datatype | Source Timestamp |
|---|---|---|---|---|---|---|
| 1 | DNA-OPCUA-S... | NS1\|String\|TEST... | av | 11 | Float | 04/10/2022 14.4... |

| Attribute | Value |
|---|---|
| NodeId | ns=1;s=TEST-AM/av |
| NamespaceIndex | 1 |
| IdentifierType | String |
| Identifier | TEST-AM/av |
| NodeClass | Variable |
| BrowseName | 0, "av" |
| DisplayName | "", "av" |
| Description | "", "" |
| Value | |
| SourceTimestamp | 04/10/2022 14.43.17 |
| SourcePicoseconds | 0 |
| ServerTimestamp | 04/10/2022 14.45.55 |
| ServerPicoseconds | 0 |
| StatusCode | Good (0x00000000) |
| Value | 11 |
| DataType | Float |
| NamespaceIndex | 0 |
| IdentifierType | Numeric |
| Identifier | 10 [Float] |
| ValueRank | -1 (Scalar) |
| ArrayDimensions | UInt32 Array[-1] |
| AccessLevel | CurrentRead, CurrentWrite, HistoryRead |
| UserAccessLevel | CurrentRead |
| AccessLevelEx | CurrentRead, CurrentWrite, HistoryRead |
| MinimumSamplingInterval | 0 |
| Historizing | true |
| WriteMask | 0 |
| UserWriteMask | 0 |
| RolePermissions | RolePermissionType Array[6] |
| UserRolePermissions | RolePermissionType Array[1] |
| [0] | RolePermissionType |
| RoleId | i=15644 [WellKnownRole_Anonymous] |
| Permissions | Browse, ReadRolePermissions, Read |
| AccessRestrictions | None |

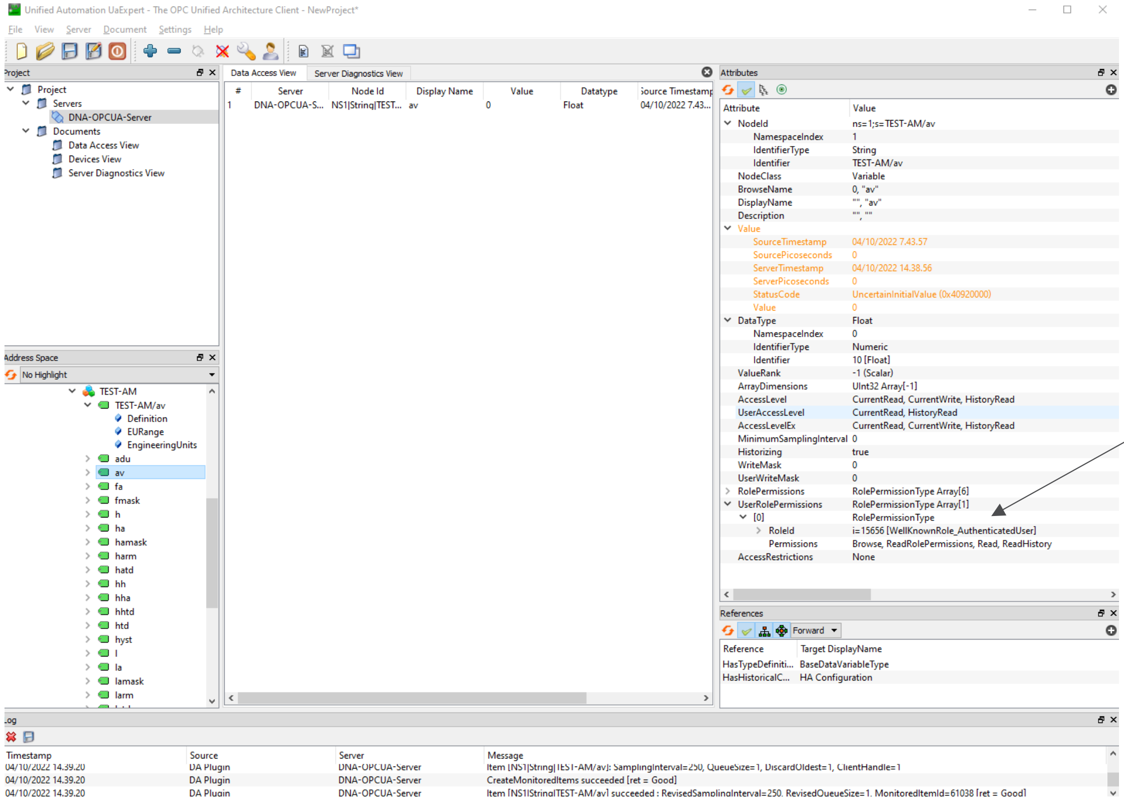
| Reference | Target DisplayName |
|---|---|
| HasTypeDefiniti... | BaseDataVariableType |
| HasHistoricalC... | HA Configuration |

```
Timestamp            Source             Server             Message
04/10/2022 14.45.55  Reference Plugin   DNA-OPCUA-Server   Browse succeeded.
04/10/2022 14.45.55  Attribute Plugin   DNA-OPCUA-Server   Read attributes of node 'NS1|String|TEST-AM/av' succeeded [ret = Good].
04/10/2022 14.45.55  Reference Plugin   DNA-OPCUA-Server   Browse succeeded.
```

Permissions:
Browse,
ReadRolePermissions,
Read

# OPC UA – Authenticated user: read-only permissions

## UaExpert



Unified Automation UaExpert - The OPC Unified Architecture Client - NewProject*
File View Server Document Settings Help
Project
Data Access View
Server Diagnostics View
Attributes
References
Forward
Address Space
No Highlight
Log

Project
- Project
  - Servers
    - DNA-OPCUA-Server
  - Documents
    - Data Access View
    - Devices View
    - Server Diagnostics View

| # | Server | Node Id | Display Name | Value | Datatype | Source Timestamp |
|---|---|---|---|---|---|---|
| 1 | DNA-OPCUA-S... | NS1\|String\|TEST... | av | 0 | Float | 04/10/2022 7.43... |

| Attribute | Value |
|---|---|
| NodeId | ns=1;s=TEST-AM/av |
| NamespaceIndex | 1 |
| IdentifierType | String |
| Identifier | TEST-AM/av |
| NodeClass | Variable |
| BrowseName | 0, "av" |
| DisplayName | "", "av" |
| Description | "", "" |
| Value | |
| SourceTimestamp | 04/10/2022 7.43.57 |
| SourcePicoseconds | 0 |
| ServerTimestamp | 04/10/2022 14.38.56 |
| ServerPicoseconds | 0 |
| StatusCode | UncertainInitialValue (0x40920000) |
| Value | 0 |
| DataType | Float |
| NamespaceIndex | 0 |
| IdentifierType | Numeric |
| Identifier | 10 [Float] |
| ValueRank | -1 (Scalar) |
| ArrayDimensions | UInt32 Array[-1] |
| AccessLevel | CurrentRead, CurrentWrite, HistoryRead |
| UserAccessLevel | CurrentRead, HistoryRead |
| AccessLevelEx | CurrentRead, CurrentWrite, HistoryRead |
| MinimumSamplingInterval | 0 |
| Historizing | true |
| WriteMask | 0 |
| UserWriteMask | 0 |
| RolePermissions | RolePermissionType Array[6] |
| UserRolePermissions | RolePermissionType Array[1] |
| [0] | RolePermissionType |
| RoleId | i=15656 [WellKnownRole_AuthenticatedUser] |
| Permissions | Browse, ReadRolePermissions, Read, ReadHistory |
| AccessRestrictions | None |

Address Space
- TEST-AM
  - TEST-AM/av
    - Definition
    - EURange
    - EngineeringUnits
  - adu
  - av
  - fa
  - fmask
  - h
  - ha
  - hamask
  - harm
  - hatd
  - hh
  - hha
  - hhtd
  - htd
  - hyst
  - l
  - la
  - lamask
  - larm

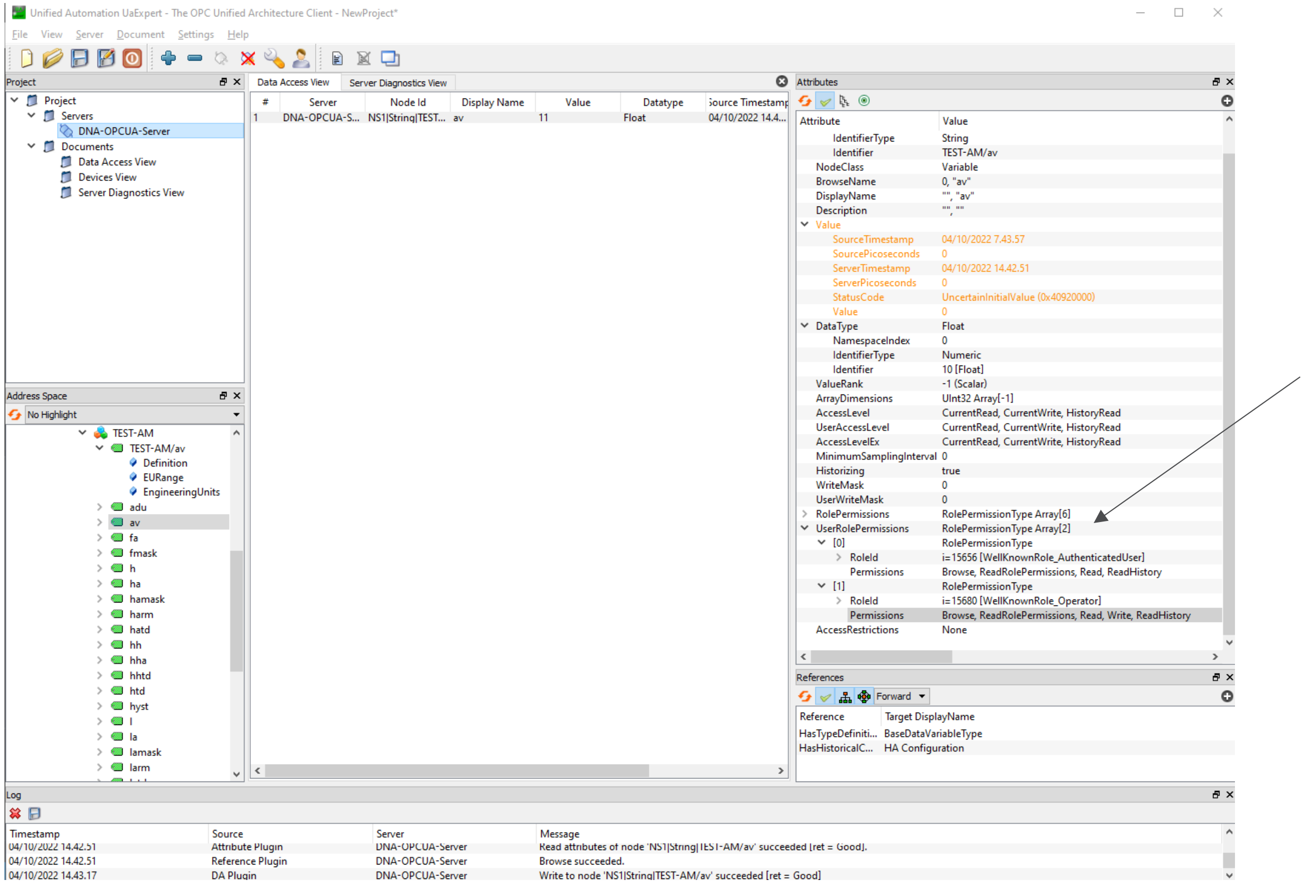
| Reference | Target DisplayName |
|---|---|
| HasTypeDefiniti... | BaseDataVariableType |
| HasHistoricalC... | HA Configuration |

```
Timestamp            Source      Server              Message
04/10/2022 14.39.20  DA Plugin   DNA-OPCUA-Server    Item [NS1|String|TEST-AM/av]: SamplingInterval=250, QueueSize=1, DiscardOldest=1, ClientHandle=1
04/10/2022 14.39.20  DA Plugin   DNA-OPCUA-Server    CreateMonitoredItems succeeded [ret = Good]
04/10/2022 14.39.20  DA Plugin   DNA-OPCUA-Server    Item [NS1|String|TEST-AM/av] succeeded : RevisedSamplingInterval=250, RevisedQueueSize=1, MonitoredItemId=61038 [ret = Good]
```

Permissions:
Browse,
ReadRolePermissions,
Read,
ReadHistory

# OPC UA – Operator: Write permission to modify values

## UaExpert



| # | Server | Node Id | Display Name | Value | Datatype | Source Timestamp |
|---|---|---|---|---|---|---|
| 1 | DNA-OPCUA-S... | NS1\|String\|TEST... | av | 11 | Float | 04/10/2022 14.4... |

| Attribute | Value |
|---|---|
| IdentifierType | String |
| Identifier | TEST-AM/av |
| NodeClass | Variable |
| BrowseName | 0, "av" |
| DisplayName | "", "av" |
| Description | "", "" |
| Value | |
| SourceTimestamp | 04/10/2022 7.43.57 |
| SourcePicoseconds | 0 |
| ServerTimestamp | 04/10/2022 14.42.51 |
| ServerPicoseconds | 0 |
| StatusCode | UncertainInitialValue (0x40920000) |
| Value | 0 |
| DataType | Float |
| NamespaceIndex | 0 |
| IdentifierType | Numeric |
| Identifier | 10 [Float] |
| ValueRank | -1 (Scalar) |
| ArrayDimensions | UInt32 Array[-1] |
| AccessLevel | CurrentRead, CurrentWrite, HistoryRead |
| UserAccessLevel | CurrentRead, CurrentWrite, HistoryRead |
| AccessLevelEx | CurrentRead, CurrentWrite, HistoryRead |
| MinimumSamplingInterval | 0 |
| Historizing | true |
| WriteMask | 0 |
| UserWriteMask | 0 |
| RolePermissions | RolePermissionType Array[6] |
| UserRolePermissions | RolePermissionType Array[2] |
| [0] | RolePermissionType |
| RoleId | i=15656 [WellKnownRole_AuthenticatedUser] |
| Permissions | Browse, ReadRolePermissions, Read, ReadHistory |
| [1] | RolePermissionType |
| RoleId | i=15680 [WellKnownRole_Operator] |
| Permissions | Browse, ReadRolePermissions, Read, Write, ReadHistory |
| AccessRestrictions | None |

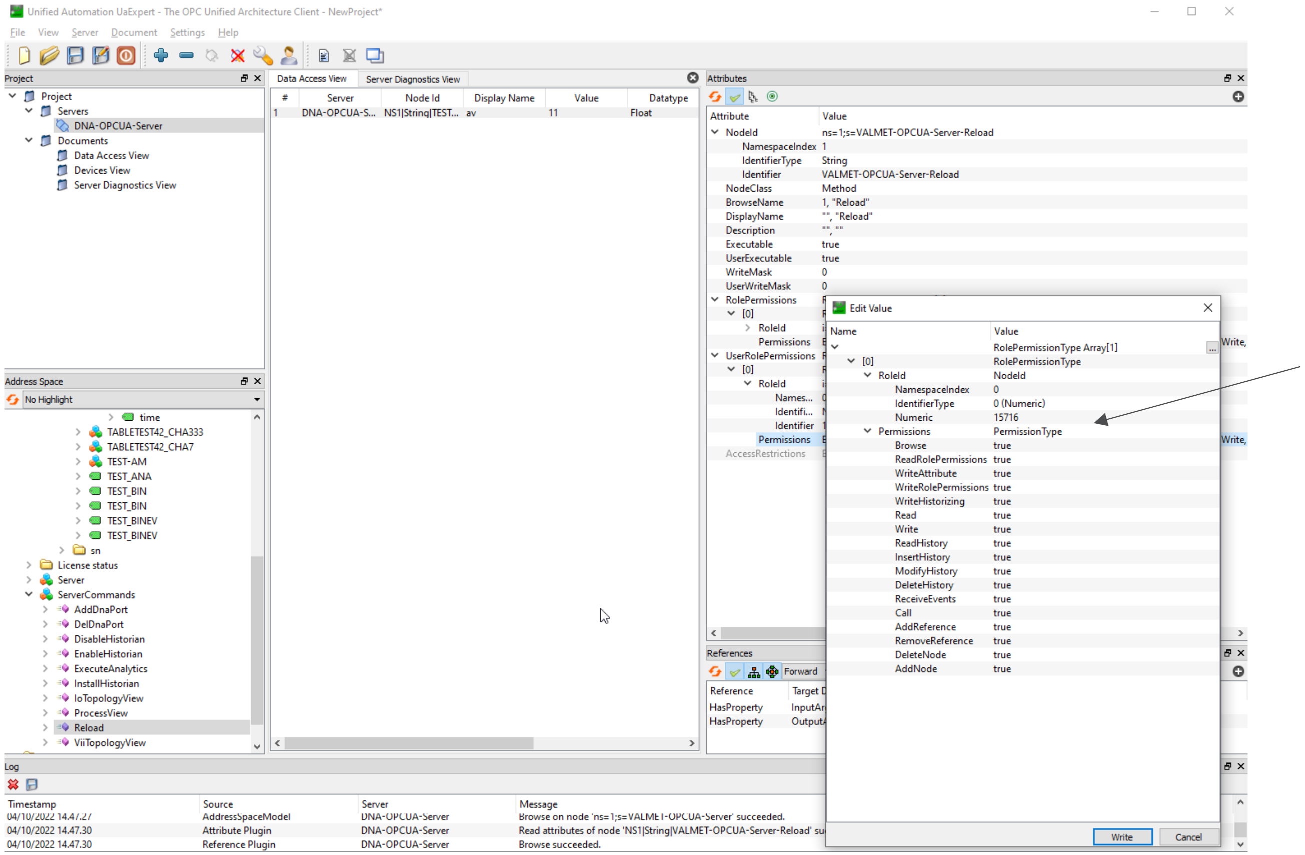
| Reference | Target DisplayName |
|---|---|
| HasTypeDefiniti... | BaseDataVariableType |
| HasHistoricalC... | HA Configuration |

| Timestamp | Source | Server | Message |
|---|---|---|---|
| 04/10/2022 14.42.51 | Attribute Plugin | DNA-OPCUA-Server | Read attributes of node 'NS1\|String\|TEST-AM/av' succeeded [ret = Good]. |
| 04/10/2022 14.42.51 | Reference Plugin | DNA-OPCUA-Server | Browse succeeded. |
| 04/10/2022 14.43.17 | DA Plugin | DNA-OPCUA-Server | Write to node 'NS1\|String\|TEST-AM/av' succeeded [ret = Good] |

Permissions:
Browse,
ReadRolePermissions,
Read,
Write,
ReadHistory

# OPC UA – Administrator: All permissions also to call methods

## UaExpert



| # | Server | Node Id | Display Name | Value | Datatype |
|---|---|---|---|---|---|
| 1 | DNA-OPCUA-S... | NS1\|String\|TEST... | av | 11 | Float |

| Attribute | Value |
|---|---|
| NodeId | ns=1;s=VALMET-OPCUA-Server-Reload |
| NamespaceIndex | 1 |
| IdentifierType | String |
| Identifier | VALMET-OPCUA-Server-Reload |
| NodeClass | Method |
| BrowseName | 1, "Reload" |
| DisplayName | "", "Reload" |
| Description | "", "" |
| Executable | true |
| UserExecutable | true |
| WriteMask | 0 |
| UserWriteMask | 0 |
| RolePermissions | |
| [0] | |
| RoleId | |
| Permissions | |
| UserRolePermissions | |
| [0] | |
| RoleId | |
| Names... | |
| Identifi... | |
| Identifier | |
| Permissions | |
| AccessRestrictions | |

| Name | Value |
|---|---|
| | RolePermissionType Array[1] |
| [0] | RolePermissionType |
| RoleId | NodeId |
| NamespaceIndex | 0 |
| IdentifierType | 0 (Numeric) |
| Numeric | 15716 |
| Permissions | PermissionType |
| Browse | true |
| ReadRolePermissions | true |
| WriteAttribute | true |
| WriteRolePermissions | true |
| WriteHistorizing | true |
| Read | true |
| Write | true |
| ReadHistory | true |
| InsertHistory | true |
| ModifyHistory | true |
| DeleteHistory | true |
| ReceiveEvents | true |
| Call | true |
| AddReference | true |
| RemoveReference | true |
| DeleteNode | true |
| AddNode | true |

| Reference | Target D |
|---|---|
| HasProperty | InputAr |
| HasProperty | OutputA |

```
Timestamp            Source               Server             Message
04/10/2022 14.47.27  AddressSpaceModel    DNA-OPCUA-Server   Browse on node 'ns=1;s=VALMET-OPCUA-Server' succeeded.
04/10/2022 14.47.30  Attribute Plugin     DNA-OPCUA-Server   Read attributes of node 'NS1|String|VALMET-OPCUA-Server-Reload' su
04/10/2022 14.47.30  Reference Plugin     DNA-OPCUA-Server   Browse succeeded.
```

Permissions:
Browse, ReadRolePermissions, Read,
Write,
ReadHistory
Call,
…

NOTE:
Only admin can browse ServerCommands

# SUMMARY – OPC UA contains a lot of features that are not yet used

- Access rights and permissions are not yet widely supported
- This leads to applications with protocol only security
- Future will need more dynamic & variable specific permissions
- Example cases:
  - Hide folder and variables under it (business case sensitive production data)
  - Special methods for server administration (only for ConfigureAdmin role)
  - Multiple device vendors, allow access/visibility to devices based on different roles

- New Business Finland project (KONE, Valmet & Wärtsilä):
  Cybersecurity Assurance for IEC62443 Based Environments CTAC
  - Target to build audit & reporting tool for security settings, access rights and permissions for OPC UA environments
    Coordinator: petri.jurmu@vtt.fi

Valmet

FORWARD