



Discover a new level of security through an  
OPEN z/VM architecture

VM Workshop

---

June 2024

# Disclaimer

Certain information in this presentation may outline Broadcom's general product direction. This presentation shall not serve to (i) affect the rights and/or obligations of Broadcom or its licensees under any existing or future license agreement or services agreement relating to any Broadcom software product; or (ii) amend any product documentation or specifications for any Broadcom software product. This presentation is based on current information and resource allocations as of June 21, 2024, and is **subject to change or withdrawal by Broadcom at any time without notice. The development, release and timing of any features or functionality described in this presentation remain at Broadcom's sole discretion.**

Notwithstanding anything in this presentation to the contrary, upon the general availability of any future Broadcom product release referenced in this presentation, Broadcom may make such release available to new licensees in the form of a regularly scheduled major product release. Such release may be made available to licensees of the product who are active subscribers to Broadcom maintenance and support, on a when and if-available basis. The information in this presentation is not deemed to be incorporated into any contract.

Copyright © 2024 Broadcom. All rights reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries. Broadcom, the pulse logo, Connecting everything, CA Technologies and the CA Technologies logo are among the trademarks of Broadcom.

**THIS PRESENTATION IS FOR YOUR INFORMATIONAL PURPOSES ONLY.** Broadcom assumes no responsibility for the accuracy or completeness of the information. TO THE EXTENT PERMITTED BY APPLICABLE LAW, BROADCOM PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. In no event will Broadcom be liable for any loss or damage, direct or indirect, in connection with this presentation, including, without limitation, lost profits, lost investment, business interruption, goodwill, or lost data, even if Broadcom is expressly advised in advance of the possibility of such damages.



**Brian Jagos**  
Client Services Consultant,  
Broadcom



**Austin Willoughby**  
Engineer,  
Broadcom

# Opening z/VM access with new APIs

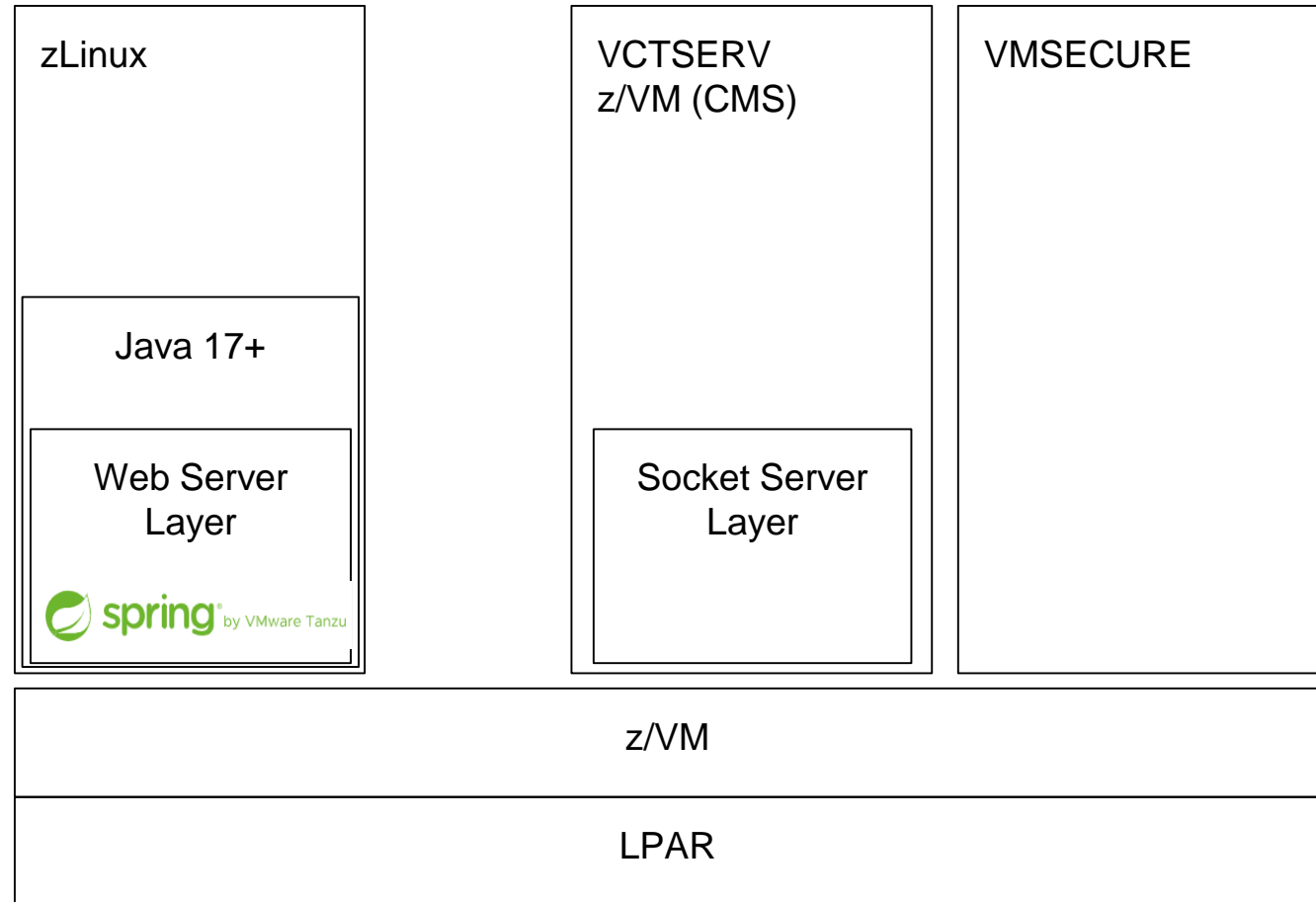
# z/VM API – a layered approach

In a z/VM system

A z/Linux guest hosts a web server  
for a Spring Boot REST service

A z/VM guest provides a socket  
server

The socket server accesses  
other guests like VM:Secure  
under the requestor's authority

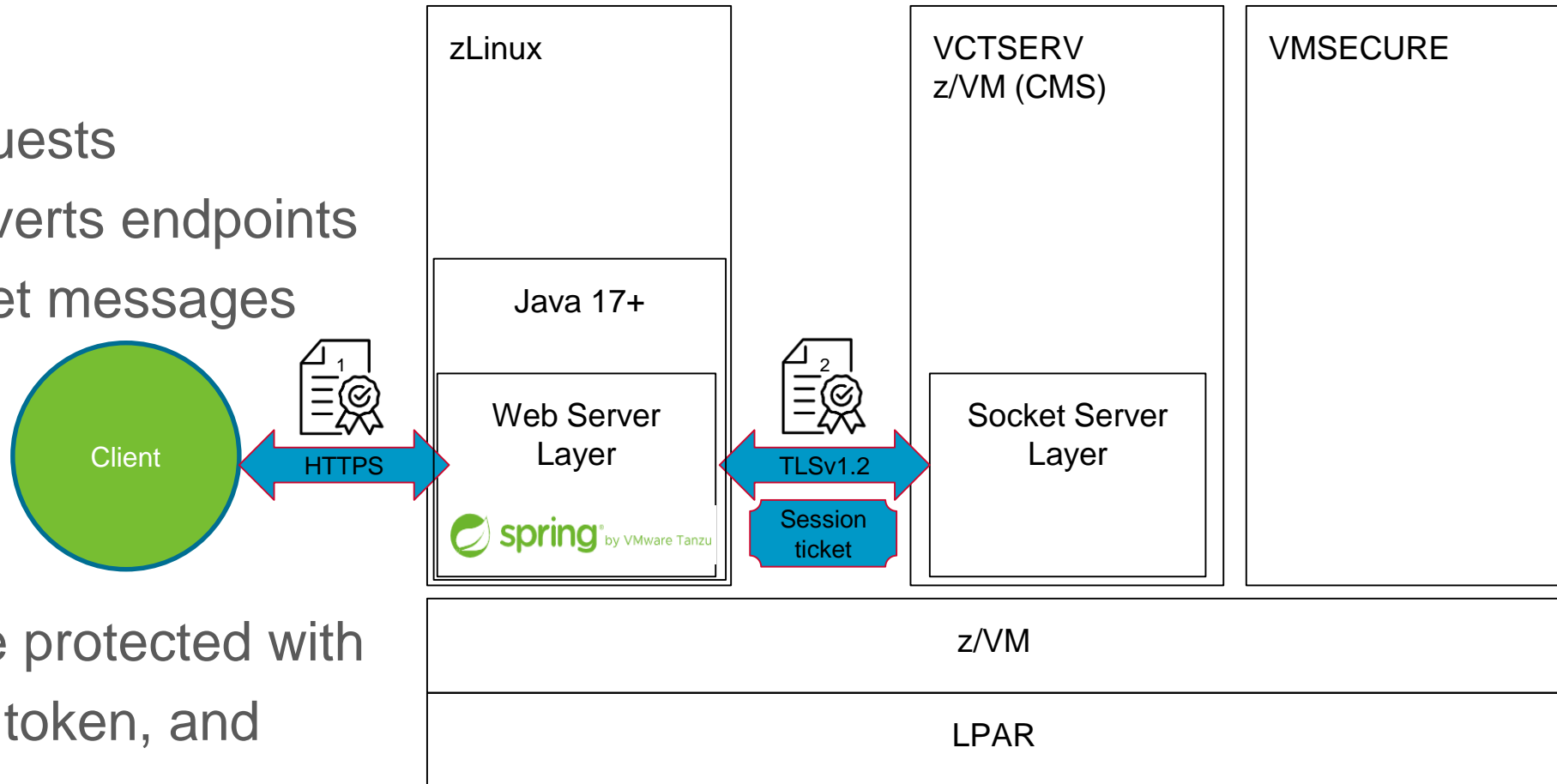


# z/VM API – connecting clients

Client solutions

make RESTful requests

The web server converts endpoints and parms to socket messages



Communications are protected with certificates, bearer token, and passtickets

# z/VM APIs Use Cases



# z/VM API Use Cases

## Privileged access management (PAM) solutions

- Symantec PAM – credential management
- Multi-Factor Authentication (MFA)
- ServiceNow Integration – approvals and ticket management
- Zero Trust Network Access (ZTNA)

## Manage user access requests

- List journal information and remove/reset journal entries
- Look for rules preventing access and delete
- Reset user password/passphrase to one-time-use value

## Manage accounts for life events

- NOLOG accounts for leave of absence

## Manage accounts for system events (maintenance)

- AUTOONLY and LBYONLY



# PAM integration

## PAM features extended to z/VM

- MFA through PAM login
  - Existing MFA implementation – RADIUS, SAML, RSA SecurID, Okta, Azure
- Credential vaulting for z/VM
- Limits attack surface
  - Threat Analytics for abnormal connection behavior
- Session management recording – playback or audit
- Password composition policies without exits
- Highly scalable and available
- Enterprise-wide, common security

# Symantec PAM 3270 logon and password rotation

The screenshot displays the Symantec Privileged Access Manager Client interface. At the top, the user is logged in as Austin Willoughby. The main section is titled "Access Devices" and includes a search bar with "Column:" and "Value:" fields, and buttons for "Filter", "Reset", "Add Filter", and "My Views". A "Restart Session" button is also present. Below this is a table with the following columns: Device Name, Address, Operati, Access Methods, Web Portal, RDP Applications, Services, and Target Applications. The table contains one entry: "zVM Test Environment" with address "zvmtest01.broadcom.net" and operation "Other". Under "Access Methods", there is a "TN3270" icon. Under "Services", there is a "TN3270 Client" icon. Under "Target Applications", there is a "Select" icon. A mouse cursor is pointing at the "Select" icon. At the bottom of the window, the footer text reads: "Symantec © 2024 Broadcom. All Rights Reserved. - 4.1.5.109 - capam".

Device Name	Address	Operati	Access Methods	Web Portal	RDP Applications	Services	Target Applications
zVM Test Environment	zvmtest01.broadcom.net	Other	TN3270			TN3270 Client	Select

# Symantec PAM password composition policy

The screenshot displays the Symantec Privileged Access Manager Client interface. A modal dialog titled "Update Password Composition Policy vmsecure" is open. At the top of the dialog, a green checkmark and the text "Confirmation: Test Passed, Sample password: TE\$32]JI" are visible. The dialog is divided into several sections:

- Name:** A text input field containing "vmsecure".
- Description:** An empty text area.
- Remote Password Generation:** A checkbox for "AWS Access Credentials" which is currently unchecked.
- Password Prefix:** An empty text input field.
- Minimum Length:** A dropdown menu set to "6".
- Maximum Length:** A dropdown menu set to "8".
- Minimum Iterations Before Reuse:** A dropdown menu set to "0".
- Minimum Days Before Reuse:** A dropdown menu set to "0".
- Maximum Password Age Enforcement:** A checked checkbox.
- Maximum Password Age Days:** A dropdown menu set to "30".
- Must Not Contain Rules:** A list of checkboxes: "Disallow Repeating Characters", "Disallow Duplicate Characters", "Disallow Max Class Repeat", and "Characters To Exclude". The "Disallow Max Class Repeat" dropdown is set to "2".
- Must Contain:** A section with three checked checkboxes: "Upper Case Characters", "Numeric Characters", and "Special Characters Including". Below these is a text input field containing the special characters string: "#\$%()\*+,-./:;=?@[\\]^\_`{|}~&".
- First Must Contain:** A section with three unchecked checkboxes: "Upper Case First Characters", "Lower Case First Characters", and "Numeric First Characters". Below these is a text input field containing the same special characters string.
- Last Must Contain:** A section with three unchecked checkboxes: "Upper Case Last Characters", "Lower Case Last Characters", and "Numeric Last Characters". Below these is a text input field containing the same special characters string.

At the bottom of the dialog, there are four buttons: "Test", "Restore Defaults", "OK", and "Cancel".

At the bottom of the main application window, the footer text reads: "Symantec. © 2024 Broadcom. All Rights Reserved. - 4.1.5.109 - capam".

# ServiceNow Integration through Symantec PAM

## Out-of-the-box integration for Symantec PAM with ServiceNow

- Vault credentials in PAM to access ServiceNow
- Create a password view policy workflow that connects to ServiceNow
  - Ticket number checked against filters like type and status (e.g. approved)
  - PAM user requesting elevated access brings the ticket number

Other service desk integrations are also supported

- CA Service Desk Manager
- HP Service Manager
- Remedy
- Salesforce Service Cloud

# ServiceNow Integration through Symantec PAM

Update Password View Policy ServiceNow

Basic Info Dual Authorization Email Notification **Service Desk**

Service Desk Integration: \* ServiceNow

ServiceNow Server: \* de[REDACTED].service-now.com

ServiceNow Application: \* ServiceNow

ServiceNow Account: \* [REDACTED]

Ticket Type: \* Incident

Query Filter (ex: status=active): status==active

ServiceNow connection information for PAM

Many filters available  
See PAM's user guide

# ServiceNow Integration through Symantec PAM

The screenshot shows the ServiceNow interface for an incident record. The browser address bar displays the URL: `dev[redacted].service-now.com/nav_to.do?uri=%2Fincident.do%3Fsys_id%3DDef4225a40a0a0b5700d0b8a790747812%26sysparm_record_target%3Dincident%26sysparm_record_row%3D44%26sysparm_record_rows%3D63`. The page title is "INC0000049 | Incident | ServiceNow". The left sidebar contains a "Filter navigator" and a list of application categories: Interaction, Now Mobile App, Service Desk, Similarity Analyzer, System Mobile, Incident, Create New, Assigned to me, Open, Open - Unassigned, Resolved, and All. The main content area shows the incident details for "Incident INC0000049". The "Number" field is highlighted with a blue callout bubble containing the text "ServiceNow incident number for active, in-progress ticket". Other fields include: Caller (redacted), Category (Network), Subcategory (-- None --), Service (empty), Configuration Item (nyc rac nas200), Short description (Network storage unavailable), and Description (Receiving error message with "network path not found."). On the right side, there are dropdown menus for State (In Progress), Impact (2 - Medium), Urgency (1 - High), Priority (2 - High), Assignment group (Hardware), and Assigned to (redacted). Buttons for "Follow", "Update", and "Related Search Results" are visible.

# ServiceNow Integration through Symantec PAM

The screenshot displays the Symantec CA Privileged Access Manager interface. The main window shows a list of devices with columns for Device Name, Address, Operating Sys, and Access Methods. A modal dialog titled 'Available Credentials' is open, displaying a table of credentials. A blue callout bubble points to the 'changeadm' credential in the table.

In PAM's Access Manager  
choose the account (e.g. changeadm)  
ServiceNow Integration prompts for  
incident number

Device Name	Access Name	Application Name	Access Mode
2020 PAM Analyst Lab - RH EL-7.5 (i-069eb639ad10f6363)	changeadm	RHEL-7.5 - UNIX	Credential Available
2020 PAM Analyst Lab - RH EL-7.5 (i-069eb639ad10f6363)	demo1	RHEL-7.5 - UNIX	Credential Available
2020 PAM Analyst Lab - RH EL-7.5 (i-069eb639ad10f6363)	demo2	RHEL-7.5 - UNIX	Credential Available
2020 PAM Analyst Lab - RH EL-7.5 (i-069eb639ad10f6363)	demokey	RHEL-7.5 - UNIX	Credential Available
2020 PAM Analyst Lab - RH EL-7.5 (i-069eb639ad10f6363)	root	RHEL-7.5 - UNIX	Credential Available



# ServiceNow Integration through Symantec PAM

PAM verifies ticket via ServiceNow using workflow query filters to allow access

Enter your ticket and comment and click OK

The screenshot displays the Symantec PAM interface. On the left, a list of sessions is visible, including '2020 PAM Analyst Lab - PAM-SC-Database' and '2020 PAM Analyst Lab - RHEL-7.2'. On the right, a 'Connect' dialog box is open, showing a dropdown menu for 'Severity 1: Manual recovery from server outage', a 'Description' field containing 'INC0000049', and a 'ServiceNow Ticket Number' field also containing 'INC0000049'. The dialog has 'OK' and 'CANCEL' buttons at the bottom right. A blue callout bubble on the left contains the text 'PAM verifies ticket via ServiceNow using workflow query filters to allow access', with a blue arrow pointing from it to the 'Connect' dialog. Another blue callout bubble on the right contains the text 'Enter your ticket and comment and click OK', with a blue arrow pointing from it to the 'OK' button in the dialog.

# ServiceNow Integration through Symantec PAM

CA Privileged Access Manager Client - 10.0.1.21



CA Privileged Access Manager

Symantec

Dashboard Access Sessions Users Services Devices Credentials Policies Settings Configuration

**Warning:** PAM-CMN-0628: An LDAP operation is in progress.

## Devices

Column:

Device Name

2020 PAM Analyst Lab - Nessus Scanner (i-0083bdac171b05686)

2020 PAM Analyst Lab - PAM-SC (i-035eb2c01c19a36b0)

2020 PAM Analyst Lab - PAM-SC-Database (i-0f9012a96c42ced61)

2020 PAM Analyst Lab - RHEL-7.2 (i-063f8530bd36cc5c5)

2020 PAM Analyst Lab - RHEL-7.5 (i-069eb639ad10f6363)

```
changeadm@ip-10-0-1-26:~  
Reminder: All actions are recorded  
Last login: Thu Sep  3 17:11:33 2020 from 10.0.1.21  
[changeadm@ip-10-0-1-26 ~]$ whoami  
changeadm  
[changeadm@ip-10-0-1-26 ~]$
```

PAM transparently logs user on without showing credentials

# Other Symantec PAM Integrations

## Integrate further with custom programming

- Ticketing systems (e.g. ServiceNow) drive processing with PAM APIs
- Out-of-the-box PAM validates tickets with outbound requests
- API programming allows ticketing systems to change PAM access
  - Ticket created to obtain maintenance account access (for time window)
  - Approvals grant access within ticketing system
  - Approval workflow uses PAM APIs to allow access and removes when window expires or ticket status changes

## Symantec PAM ZTNA integration

- ZTNA (Zero Trust Network Access) – previously Secure Access Cloud (SAC)
- Securely access systems by limiting remote user systems based on authorization
  - Secure tunnel for PAM access without VPNs or virtual desktops
  - Users ↔ ssh ↔ ZTNA ↔ tcp ↔ PAM ↔ 3270 ↔ z/VM
  - Web verify ssh connection, PAM MFA logon, users see only PAM access systems
  - PAM can record and audit access

# User Access Issues – Helpdesk

Users contact for z/VM login problems

Helpdesk uses tooling built with VM:Secure RESTful endpoints to determine problem

- Is the user “Journaled Out”? [sites without user exits]
- Does a VM:Secure REJECT rule exist? [sites with user exits]

Helpdesk removes journal entries for the user and deletes any REJECT rules related to the user logon

- Helpdesk doesn't need to know/remember VM:Secure command syntax
- APIs set guardrails for helpdesk functions/ability
- Basic resets can be done without senior sysprogs

## Password resets – Next step

The journal entries are removed and no rules prevent logon, but the user has forgotten their password

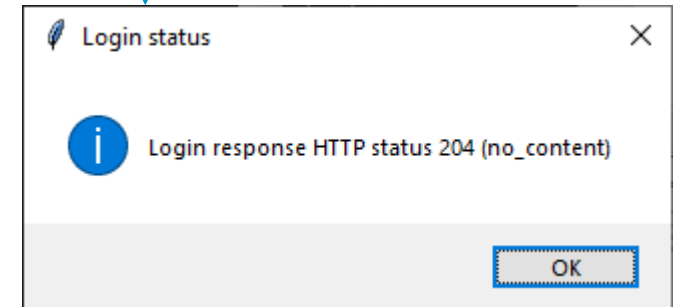
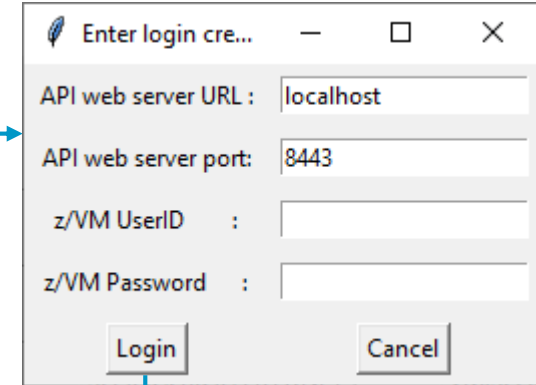
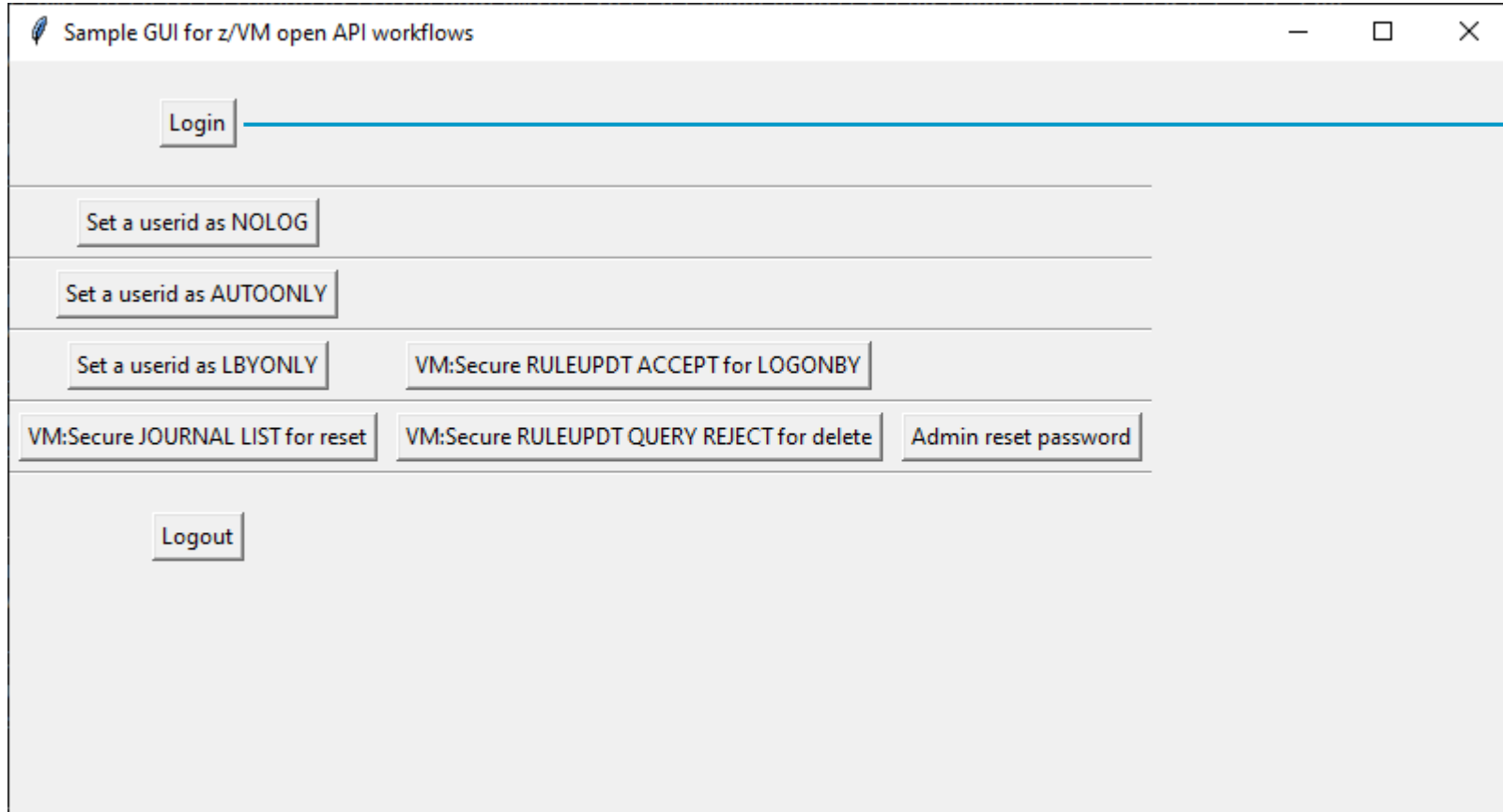
Helpdesk sets a new password that requires reset

- Random password can be set by tooling
- Password can be sent via text or email so helpdesk never sees it
- User can login 3270 and is forced to change password on first logon

PAM credential manager resets password (out-of-sync)

- Sets a known value
- Uses login endpoint to change to a new password to reset
- Session management can seamlessly logon user

# API authentication demo



# Authentication Query Details

Endpoint:

<https://localhost:8443/api/v1/auth/query>

Cookie: XSRF-TOKEN (cross-site request forgery token)

Subsequent requests include token as value for session header: X-XSRF-TOKEN

**GET** /api/v1/auth/query Validate the token and return token details

**Parameters**

No parameters

**Responses**

Code	Description
200	Successful validation
	Media type <input type="text" value="application/json"/>
	Controls Accept header.
	Example Value   Schema
	<pre>{   "creation": "2024-06-07T13:51:42.873Z",   "expiration": "2024-06-07T13:51:42.873Z",   "userId": "string" }</pre>
401	Invalid credentials



# Authentication Login Details

Endpoint:

<https://localhost:8443/api/v1/auth/login>

Request body:

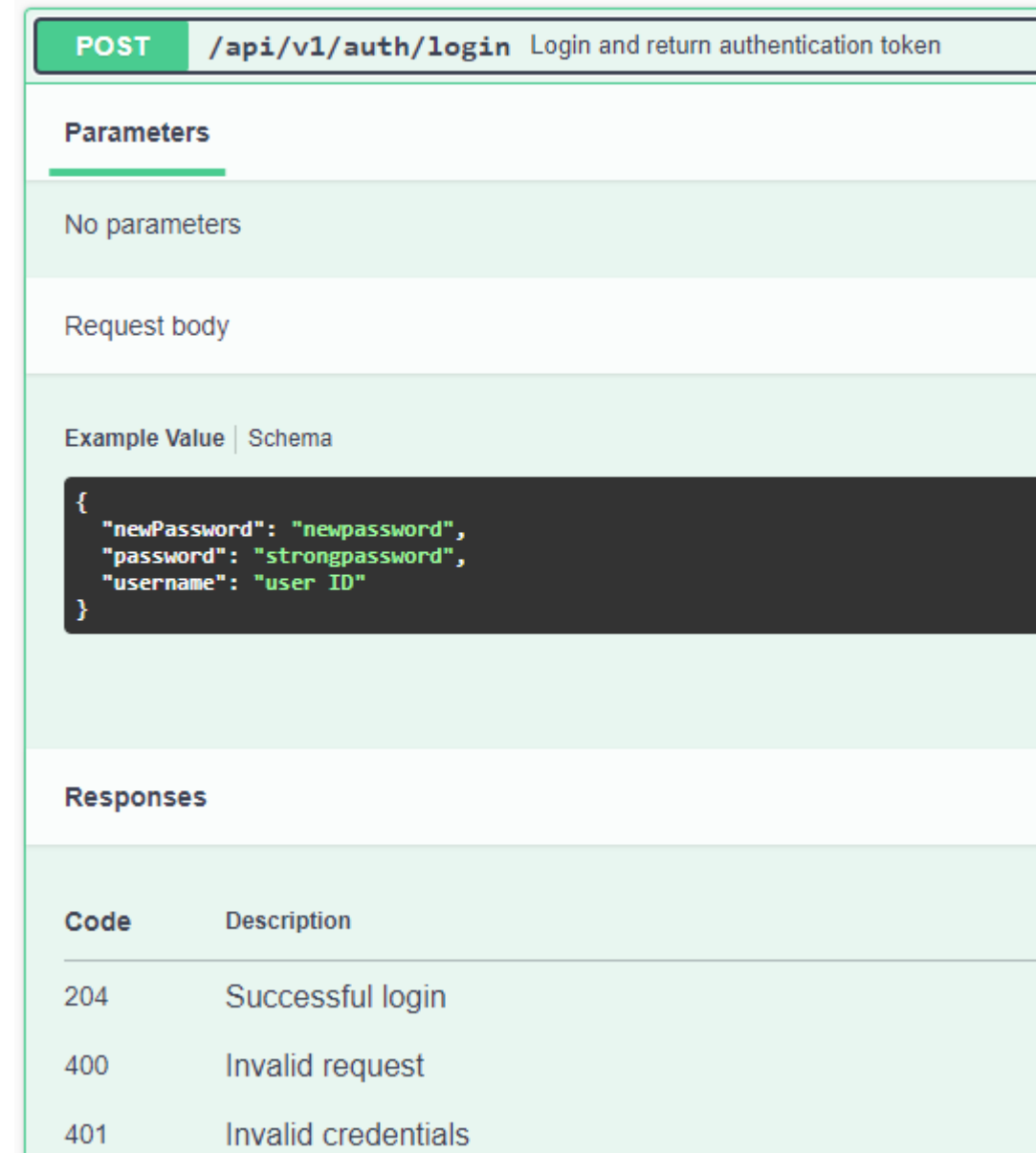
Include newPassword to change known password

z/VM rules:

API users must be enabled with a rule  
`ACCEPT <userid> <entity>`

<userid> is the API user

<entity> is API usage resource name



The image shows a snippet of API documentation for a POST endpoint. The endpoint is `/api/v1/auth/login` with the description "Login and return authentication token". Under the "Parameters" section, it states "No parameters". Under the "Request body" section, there is a table with two columns: "Example Value" and "Schema". The "Example Value" column contains a JSON object: `{ "newPassword": "newpassword", "password": "strongpassword", "username": "user ID" }`. Under the "Responses" section, there is a table with two columns: "Code" and "Description". The table lists three response codes: 204 (Successful login), 400 (Invalid request), and 401 (Invalid credentials).

Code	Description
204	Successful login
400	Invalid request
401	Invalid credentials

# User access reset steps – Journal reset

The screenshot illustrates the steps to reset journal entries in a web application. A dialog box titled "Choose a journal entry to reset" is open, showing two entries:

- Reset journal entry {"count": 1, "userOrTerm": "\*", "command": "LOGON TESTUSR1"}
- Reset journal entry {"count": 1, "userOrTerm": "127.0.0.1 5", "command": "LOGON \*"}

Buttons for "Set a...", "Set a us...", and "Set a u..." are visible on the left. Below the dialog, there are tabs for "VM:Secure JOURNAL LIST for reset", "VM:Secure RULEOPDT QUERY REJECT for delete", and "Admin reset password". A "Logout" button is also present.

Two confirmation dialogs are shown on the right, both titled "Reset status for entry...". The first dialog shows the message "Logout response HTTP status 200 (ok)" and an "OK" button. The second dialog shows the message "Logout response HTTP status 200 (ok)" and an "OK" button.

# List Journal Details

Endpoint:

<https://localhost:8443/zvmopen/api/v1/vmsecure/journal/list>

Http status codes: 200, 404 (no journal records)

z/VM authority:

The journal command should be restricted to administrative users

```
GRANT JOURNAL TO <userid>
```

```
GRANT NOPASS TO <userid>
```

<userid> is the API user

**GET** /zvmopen/api/v1/vmsecure/journal/list VM:Secure list journal

Displays current journal information.

**Parameters**

Name	Description
<b>target</b> * required string (query)	Target guest name Default value : VMSECURE

**Responses**

Code	Description
200	Successful

Media type: application/json

Controls Accept header.

Example Value | Schema

```
{
  "vmReturnCode": 0,
  "vmReasonCode": 0,
  "journalEntries": [
    {
      "count": 1,
      "userOrTerm": "*",
      "command": "LOGON TESTUSR1"
    },
    {
      "count": 1,
      "userOrTerm": "127.0.0.1",
      "command": "LOGON *"
    }
  ]
}
```

# Reset Journal Details

Endpoint:

<https://localhost:8443/zvmopen/api/v1/vmsecure/journal/reset>

**DELETE** /zvmopen/api/v1/vmsecure/journal/reset VM:Secure journal reset

Removes any journal entries that exactly match the specified variables.

**Parameters**

Request body

Example Value | Schema

```
{
  "command": "string",
  "count": 0,
  "userOrTerm": "string"
}
```

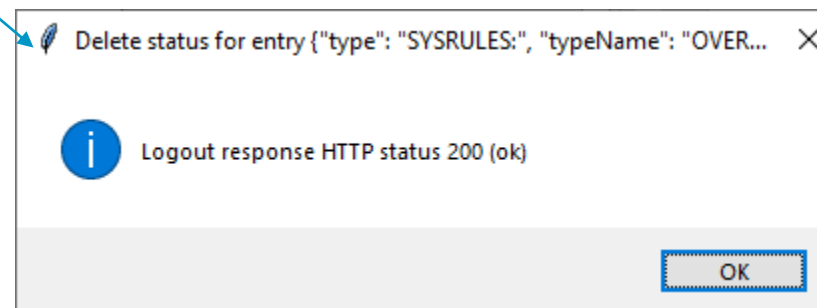
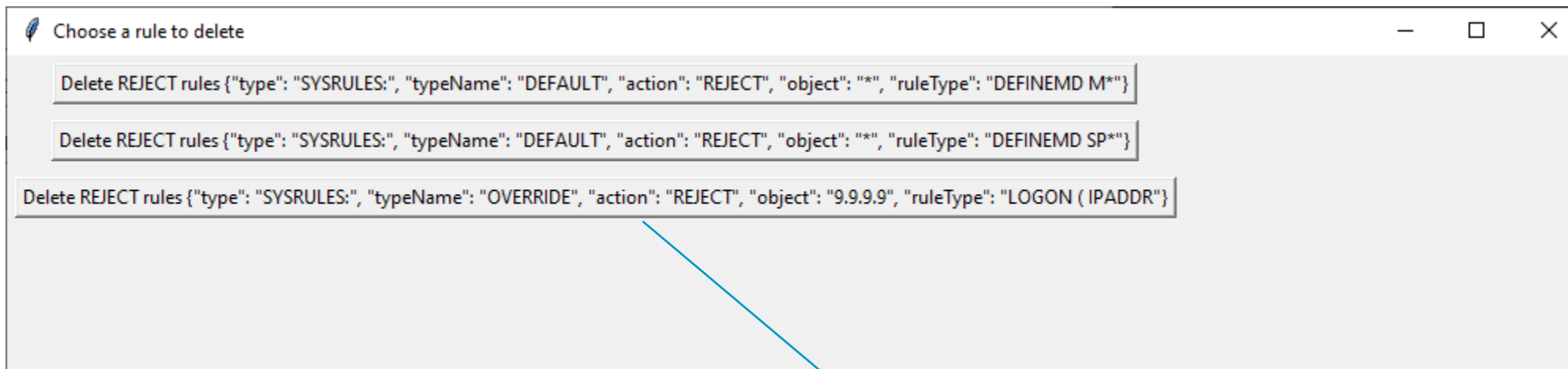
Request body:

JSON (element of journal/list response)

z/VM authority:

Same as journal/list

# RULEUPDT QUERY and DELETE



# RULEUPDT QUERY details

Endpoint: <https://localhost:8443/zvmopen/api/v1/vmsecure/query/all>

**GET** /zvmopen/api/v1/vmsecure/ruleupdt/query/all VM:Secure rule update query all

Use the RULEUPDT command to query VM:Secure rules.

**Parameters**

Name	Description
<b>target</b> * required string (query)	Target guest name Default value : VMSECURE <input type="text" value="VMSECURE"/>
ruleActionToSearch string (query)	ruleActionToSearch - ACCEPT   REJECT   * <input type="text" value="ruleActionToSearch"/>

Http status codes: 200, 404 (no rules)

Parameters:

[ruleActionToSearch=REJECT](#)

[objectToSearchFor=\\*](#)

[ruletypeToSearchFor=\\*](#)

z/VM authority:

The ruleupdt command should be restricted to administrative users

```
GRANT RULEUPDT TO <userid>
```

```
GRANT NOPASS TO <userid>
```

<userid> is the API user

# RULEUPDT DELETE details

Endpoint: <https://localhost:8443/zvmopen/api/v1/vmsecure/delete/system>

Http status codes: 200

Request body from ruleupdt query

z/VM authority: Same as query/all

**DELETE** /zvmopen/api/v1/vmsecure/ruleupdt/delete/system VM:Secure rule update delete system

Use the RULEUPDT command to delete VM:Secure SYSTEM rules.

**Parameters**

Name	Description
<b>target</b> * required	Target guest name

Request body

Example Value | Schema

```
{
  "action": "REJECT",
  "object": "*",
  "ruleType": "DEFINEMD M*",
  "type": "SYSRULES",
  "typeName": "DEFAULT"
}
```



# Admin set password

Enter account to reset the password

z/VM UserID to reset:

Password reset status

**i** Reset response HTTP status 200 (ok)  
The temporary password for user testusr1 is x9iNwemA

# Set Password to temp value

Endpoint: <https://localhost:8443/zvmopen/api/v1/password/set/testusr1>

**PUT** /zvmopen/api/v1/password/set/{userid} Sets the virtual machine specified by userid to have the specified password.

Set a password for userid.

**Parameters**

Name	Description
<b>userid</b> * required string (path)	<input type="text" value="userid"/>
newPassword string(\$password) (query)	<input type="text" value="newPassword"/>

Request body:

```
{ newPassword = "x9iNwemA" }
```

z/VM authority:

Restrict to administrative users  
vmsecure ruleuptd system add top  
'accept <admnuser> passchg (  
nopass'

# Password set for TESTUSR1 reset during logon

```
LOGON TESTUSR1
VMXACJ0171I CP command 'LOGON TESTUSR1 '
VMXACJ0172I Accepted via system rule: ACCEPT * LOGON (IPADDR HISTORY
VMXFOR0475I Your logon password has been changed.
VMXFOR0372R Select and enter a new password for your userid (LOGOFF to exit):
```

# Leave Of Absence workflow for z/VM IDs

Employee starting extended leave

- Has z/VM accounts
- Expected to return and z/VM accounts should be retained until they rejoin
- Site wants to ensure no access to the user account occurs

The site's LOA workflow is extended to set the user's z/VM accounts are set as NOLOG

The site's onboarding workflow for these users re-enables logon for their z/VM accounts

- Follows the admin set password shown
- User logons with temporary password and resets password

VM:Secure can put users on hold but might lose links

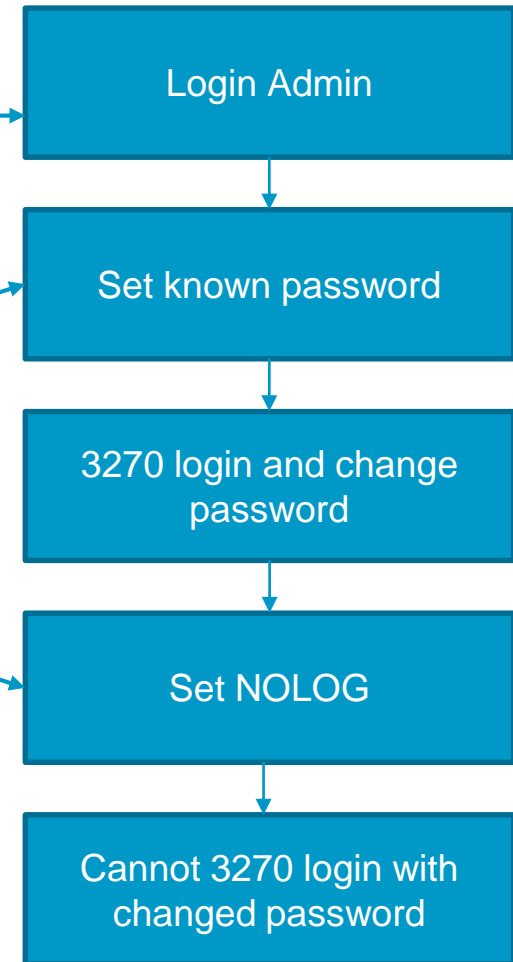
- NOLOG keeps user in directory while protecting resources (no logon)

Similar workflow for NOLOG allows cybersecurity to address suspicious activity while reviewing

- NOLOG locks down accounts and can be done quickly with an automated response

# Reset to active account, then set NOLOG

The screenshot displays the 'Sample GUI for z/VM open API workflows' with several workflow buttons: Login, Set a userid as NOLOG, Set a userid as AUTOONLY, Set a userid as LBYONLY, VM:Secure RULEUPDT ACCEPT for LOGONBY, VM:Secure JOURNAL LIST for reset, VM:Secure RULEUPDT QUERY REJECT for delete, Admin reset password, and Logout. Two modal windows are open: 'Enter account to set as NOLOG' with 'z/VM UserID to set: testusr1' and 'Set NOLOG' button; and 'Set NOLOG status' with 'Set NOLOG response HTTP status 200 (ok)' and 'OK' button.



# Set user to NOLOG

Endpoint: <https://localhost:8443/zvmopen/api/v1/password/nolog/testusr1>

z/VM authority: Same as password/set endpoint

**PUT** `/zvmopen/api/v1/password/nolog/{userid}` Sets the virtual machine specified by userid to be disallowed from access through the LOGON command.

Set the NOLOG special password to prevent use of the LOGON command to log on the ID.

### Parameters

Name	Description
<b>userid</b> * required string	<input type="text" value="userid"/>

# Maintenance for service machines – Simple and Secure

A service machine requires a configuration change

- Example: TESTDSM requires a change and is AUTOONLY or LBYONLY
- The maintenance user must logon TESTDSM or LOGON BY

Maintenance enabled for AUTOONLY

- Reset TESTDSM password at start of maintenance using password reset workflow to assign a temporary password
- The user logs on through 3270 and does maintenance activity
- When complete, TESTDSM set to AUTOONLY

Maintenance enabled for LBYONLY

- A service machine can be set to LBYONLY or already is
- A rule is created to allow the user to LOGON BY to the service machine
- The rule expires

Site policy says all service machines must be set as AUTOONLY to prevent direct logon

- An administrator can run the endpoint multiple times for different service machines



# Maintenance AUTOONLY service machine

The screenshot displays a web application interface titled "Sample GUI for z/VM open API workflows". The main interface contains several buttons for user management: "Login", "Set a userid as NOLOG", "Set a userid as AUTOONLY", "Set a userid as LBYONLY", "VM:Secure RULEUPDT ACCEPT for LOGONBY", "VM:Secure JOURNAL LIST for reset", "VM:Secure RULEUPDT QUERY REJECT for delete", and "Admin reset password". A "Logout" button is also present.

A blue arrow points from the "Set a userid as AUTOONLY" button to a modal dialog box titled "Enter account to set as AUTOONLY". This dialog has a text input field labeled "z/VM UserID to set:" containing the text "testdsm". Below the input field are two buttons: "Set AUTOONLY" and "Cancel".

Another blue arrow points from the "Set AUTOONLY" button in the modal to a second modal dialog box titled "Set AUTOONLY status". This dialog features an information icon and the text "Set AUTOONLY response HTTP status 200 (ok)". An "OK" button is located at the bottom right of this dialog.

# Set user to AUTOONLY

Endpoint: <https://localhost:8443/zvmopen/api/v1/password/autoonly/testdsm>

z/VM authority: Same as password/set endpoint

**PUT** `/zvmopen/api/v1/password/autoonly/{userid}` Sets the virtual machine specified by userid to be autologged, but not logged on at a terminal.

Set the AUTOONLY special password to enable the userid to be autologged, but not logged on at a terminal.

**Parameters**

Name	Description
<b>userid</b> * required string	<input type="text" value="userid"/>

# Maintenance LBYONLY service machine

Sample GUI for z/VM open API workflows

Login

Set a userid as NOLOG

Set a userid as AUTOONLY

Set a userid as LBYONLY

VM:Secure RULEUPDT ACCEPT for LOGONBY

VM:Secure JOURNAL LIST for reset

VM:Secure RULEUPDT QUERY REJECT for delete

Admin reset password

Logout

Enter information for new V...

User to logon to (target account): testdsm

User to allow to LOGONBY target : testusr1

Expiration date and time : EXPIRE 12/31/24 23:59:!

Add LOGONBY rule

Cancel

Enter account to set as LBYONLY

z/VM UserID to set: testdsm

Set LBYONLY

Cancel

Add status

Add rule LBYONLY response HTTP status 200 (ok)

OK

Set LBYONLY status

Set LBYONLY response HTTP status 200 (ok)

OK

# Set user to LBYONLY

Endpoint: <https://localhost:8443/zvmopen/api/v1/password/lbyonly/testdsm>

z/VM authority: Same as password/set endpoint

**PUT** `/zvmopen/api/v1/password/lbyonly/{userid}` Sets the virtual machine specified by `userid` to require the LOGON command's BY option.

Set the LBYONLY special password to increase the accountability of access to shared IDs such as MAINT or VMANAGER.

**Parameters**

Name	Description
<b>userid</b> * required string	<input type="text" value="userid"/>

# Add VM:Secure rule for LOGONBY

Endpoint: <https://localhost:8443/zvmopen/api/v1/vmsecure/ruleupdt/add/user>

z/VM authority:  
Same as ruleupdt query

**POST** /zvmopen/api/v1/vmsecure/ruleupdt/add/user/{userid} VM:Secure rule update add user

Use the RULEUPDT command to add a VM:Secure USER rule.

### Parameters

Name	Description
<b>target</b> * required string (query)	Target guest name Default value : VMSECURE
rule string (query)	rule - Rule statement

VMSECURE

rule

# Authentication Logout Details

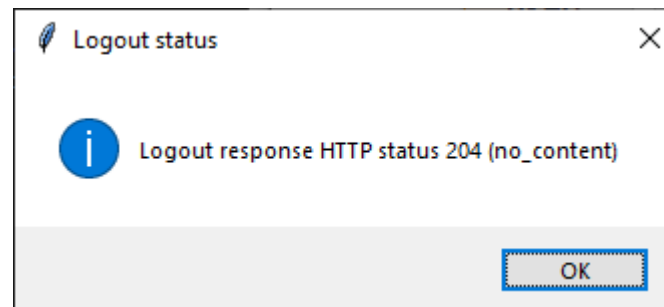
Endpoint:

<https://localhost:8443/api/v1/auth/logout>

Invalidates JWT

Invalidates z/VM Passticket

POST /api/v1/auth/logout Logout JWT token	
<b>Parameters</b>	
No parameters	
<b>Responses</b>	
Code	Description
204	Successful logout



# Open API Value

Build interfaces to help next generation users maintain without breaking

- Dashboards help users investigate, debug, maintain
  - Distribute workloads while mitigating risks from less knowledgeable users
  - Separate tasks from VM syntax and avoid mistakes
- Automate repeatable tasks to free time for senior sysprogs
  - Password resets through authorized workflows that use elevated authority
  - Integration with ticketing systems
  - See journal entries and rules that might prevent logins

Open APIs allow new access for next gen using familiar, expected tools

- Integrate existing tools with RESTful interfaces
- Modernize in-place without disruption

# Let us know

Where are your production systems in the Java lifecycle?

- Are you prepared for services requiring Java 17 or 21?

What are your use cases?

- What endpoints allow you to integrate z/VM into your enterprise solutions?
- Are there product command endpoints we can prioritize for your solutions?

What are your pain points?

- What issues would prevent you from deploying the solution?

Can you provide endpoint feedback?

- Access to the support portal for OpenAPI documentation
- Do you require passwords for users entering commands? NOPASS or implicit NOPASS

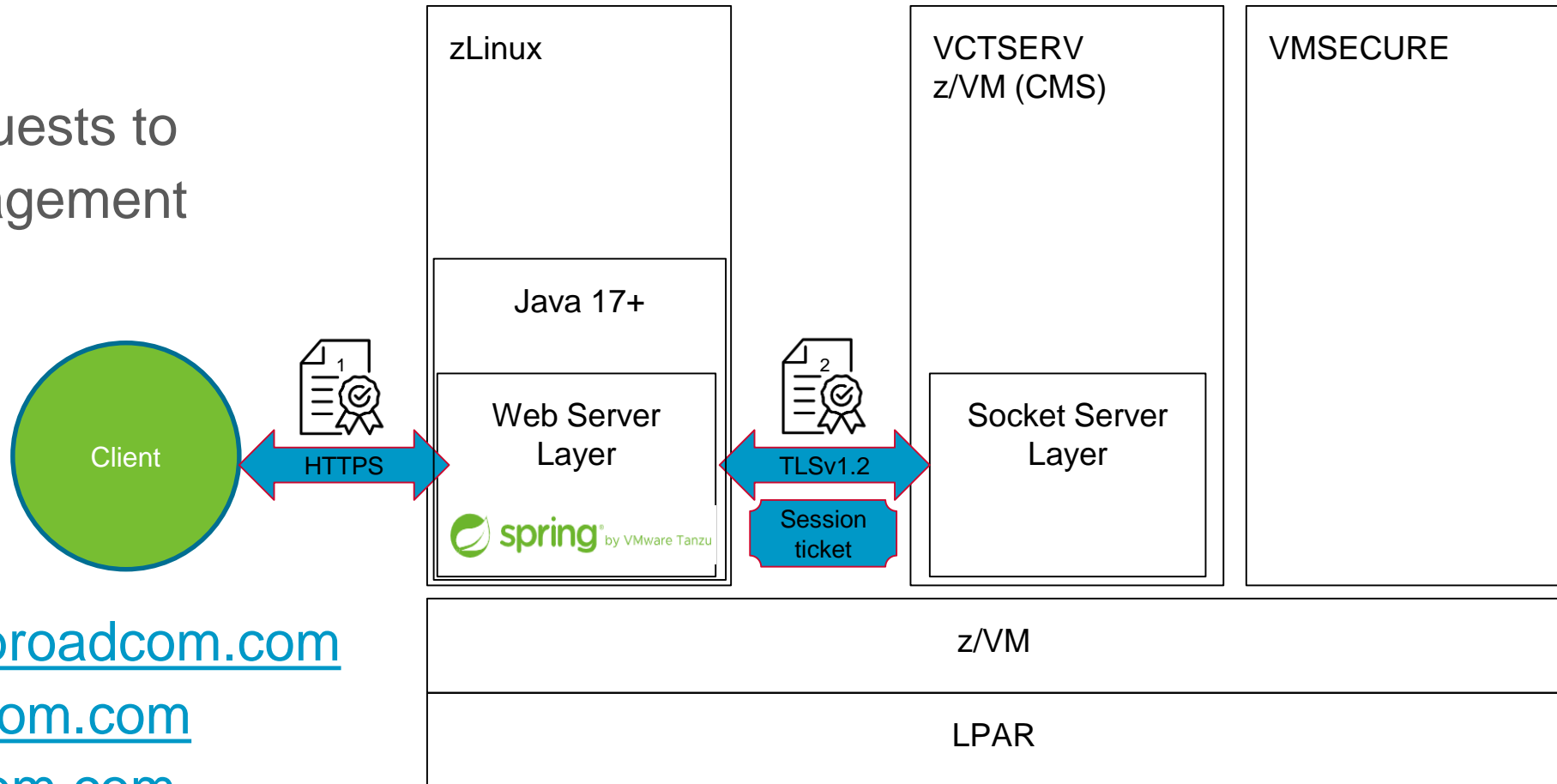




**THANK YOU**

# z/VM Open API

Client solutions  
make RESTful requests to  
Broadcom VM Management  
Products



Contacts:  
[austin.willoughby@broadcom.com](mailto:austin.willoughby@broadcom.com)  
[brian.jagos@broadcom.com](mailto:brian.jagos@broadcom.com)  
[jay.zelnick@broadcom.com](mailto:jay.zelnick@broadcom.com)