Cloud Expert

Amazon Web Services

PXL DIGITAL

AWS System Tools

AWS Systems Manager

PXL DIGITAL

“A collection of capabilities to help you manage your applications and infrastructure running in the AWS Cloud. Systems Manager simplifies application and resource management, shortens the time to detect and resolve operational problems, and helps you manage your AWS resources securely at scale.”

AWS Systems Manager

Centrally manage hybrid cloud resources at any scale

Any Environment

Operate any AWS or external resource centrally

Open

Agent is open-sourced on GitHub

Multi-platform

Windows and Linux support

Automated

Multi-account, multi-region automation

aws

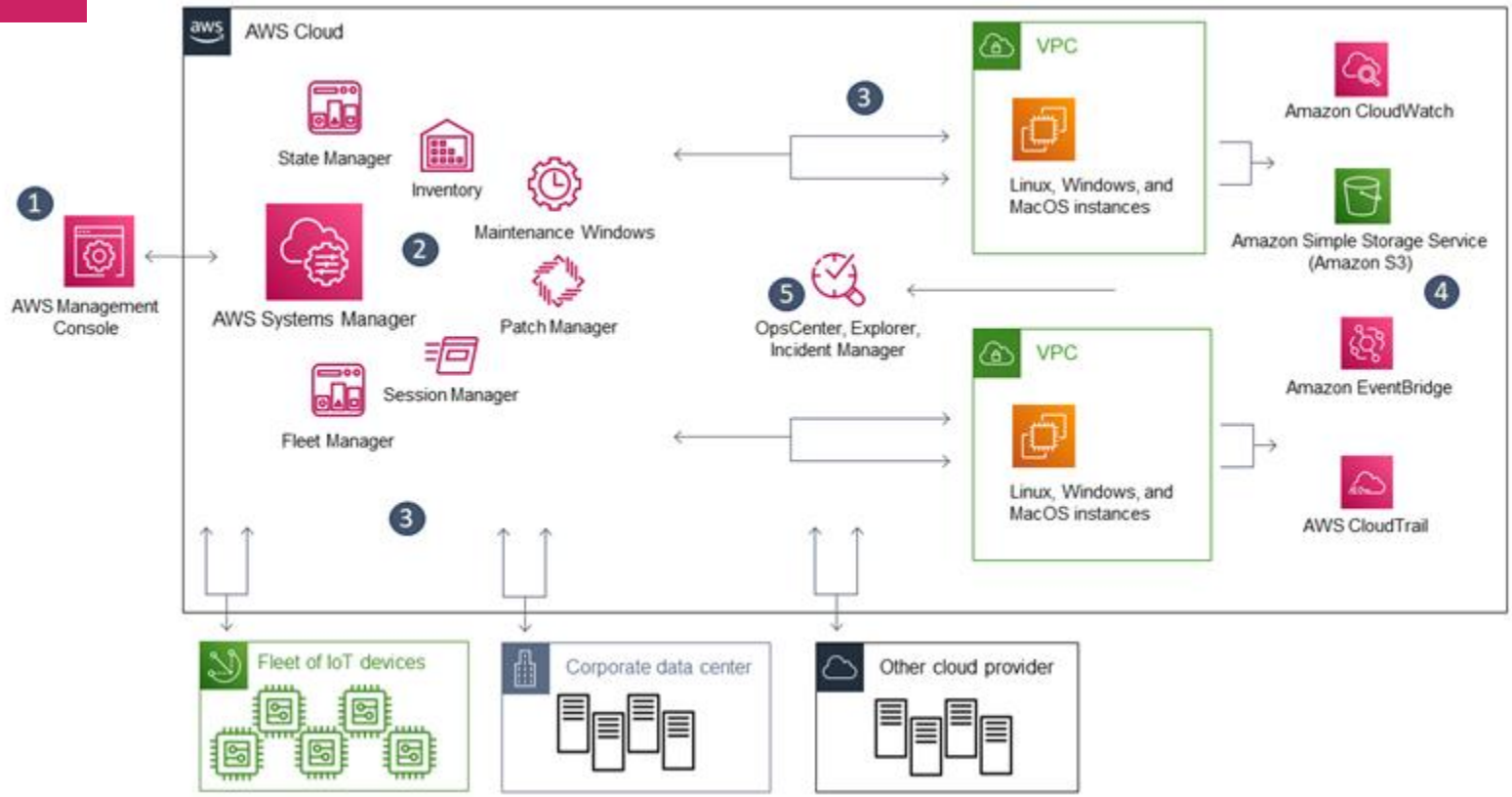
AWS Systems Manager

PXL DIGITAL

- Explorer
- OpsCenter
- Incident Manager
- Application Manager
- AppConfig
- Parameter Store
- Change Manager
- Automation
- Maintenance Windows
- Fleet Manager
- Compliance
- Inventory
- Session Manager
- Run Command
- State Manager
- Patch Manager
- Distributor

cloudar

AWS Systems Manager



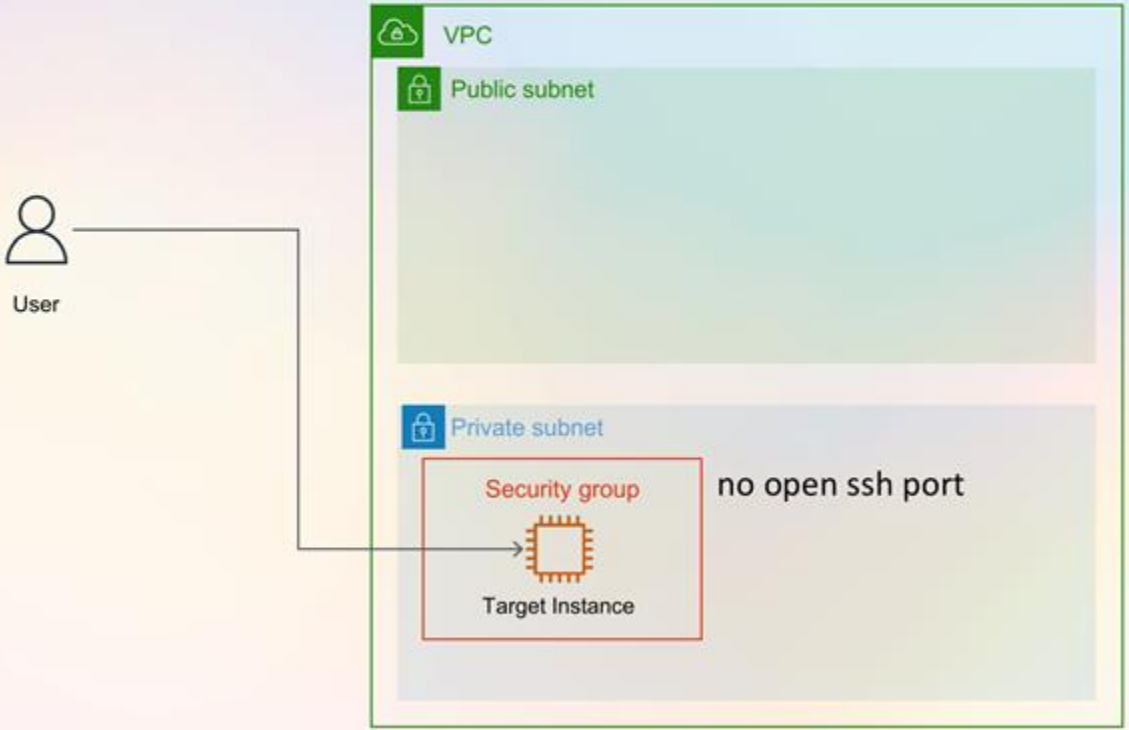
AWS Systems Manager

PXL DIGITAL

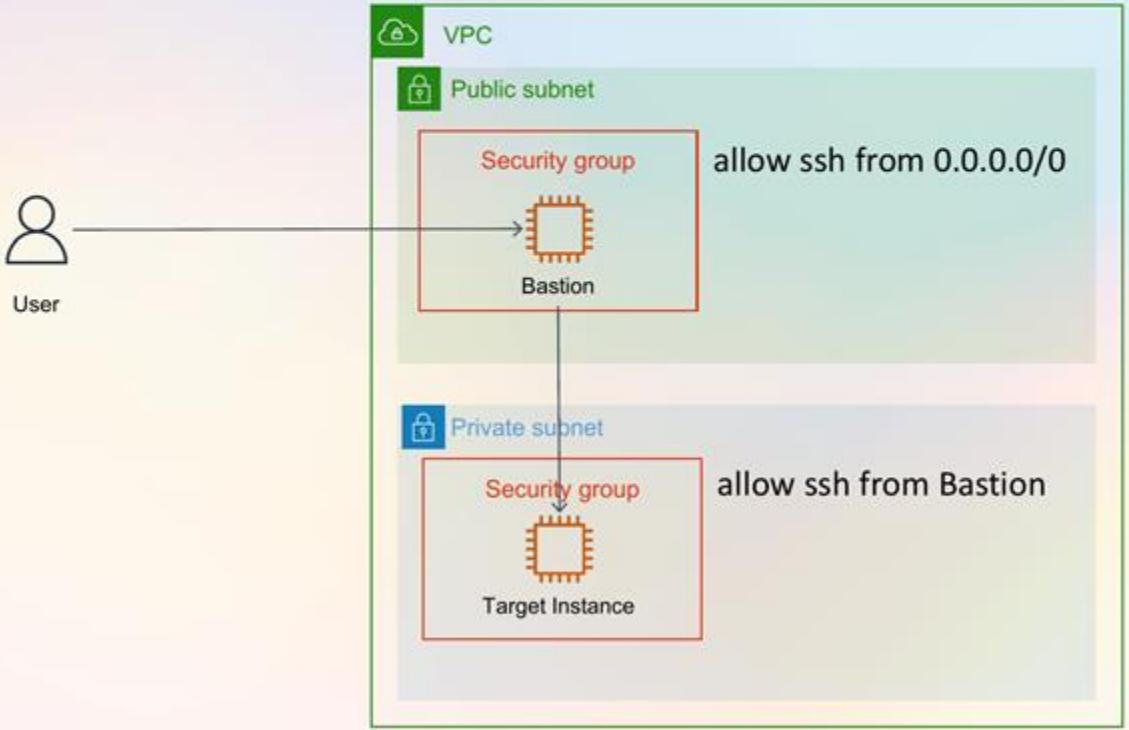
- Operations Management
  - Explorer
  - **OpsCenter**
  - Incident Manager
- Application Management
  - Application Manager
  - AppConfig
  - **Parameter Store**
- Change Management
  - Change Manager
  - **Automation**
  - Maintenance Windows
- Node Management
  - Fleet Manager
  - Compliance
  - Inventory
  - **Session Manager**
  - Run Command
  - State Manager
  - Patch Manager
  - Distributor

cloudar

Session Manager



Session Manager



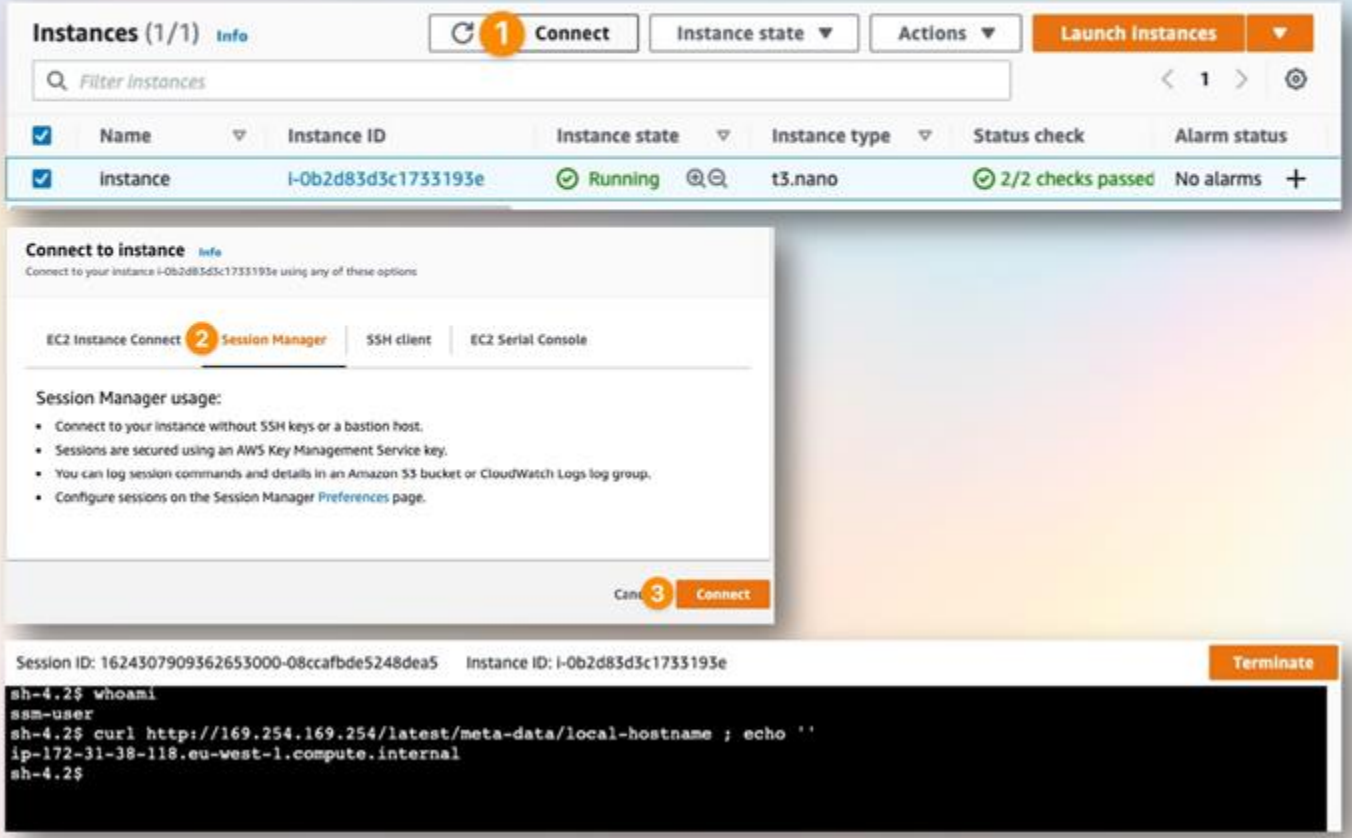
What do I need?

PXL DIGITAL

- SSM Agent
  - Installed by default on Amazon Linux, macOS, Ubuntu, Windows
  - Supports Linux, Windows, macOS
  - EC2 or Hybrid (“advanced instances”)
- IAM Role with AmazonSSMManagedInstanceCore policy
  - Or custom policy

cloudar

How does it work?



Advanced Features

PXL DIGITAL

- Use IAM permissions to control access

```
{
    "Effect": "Allow",
    "Action": [
        "ssm:StartSession"
    ],
    "Resource": [
        "arn:aws:ec2:region:account-id:instance/instance-id",
        "arn:aws:ssm:region:account-id:document/SSM-SessionManagerRunShell"
    ]
}
```

cloudar

Advanced Features

PXL DIGITAL

- Use IAM permissions to control access
- Port forwarding

```
~$ aws ssm start-session \
  --target 'i-0b2d83d3c1733193e' \
  --document-name 'AWS-StartPortForwardingSession' \
  --parameters '{"portNumber":["3389"], "localPortNumber":["9001"]}'

Starting session with SessionId: BenAtCloudar-01abdff8c6fb81427
Port 9001 opened for sessionId BenAtCloudar-01abdff8c6fb81427.
Waiting for connections...
```

cloudar

Advanced Features

PXL DIGITAL

- Use IAM permissions to control access
- Port forwarding + SSH (and SCP)

```
~$ ssh \
  -i ~/.ssh/id_rsa \
  -o ProxyCommand='sh -c "aws ssm start-session \
    --target %h \
    --document-name AWS-StartSSHSession \
    --parameters portNumber\=%p"' \
  ec2-user@i-0b2d83d3c1733193e
Last login: Mon Jun 12 17:55:53 2021 from localhost

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|
```

cloudar

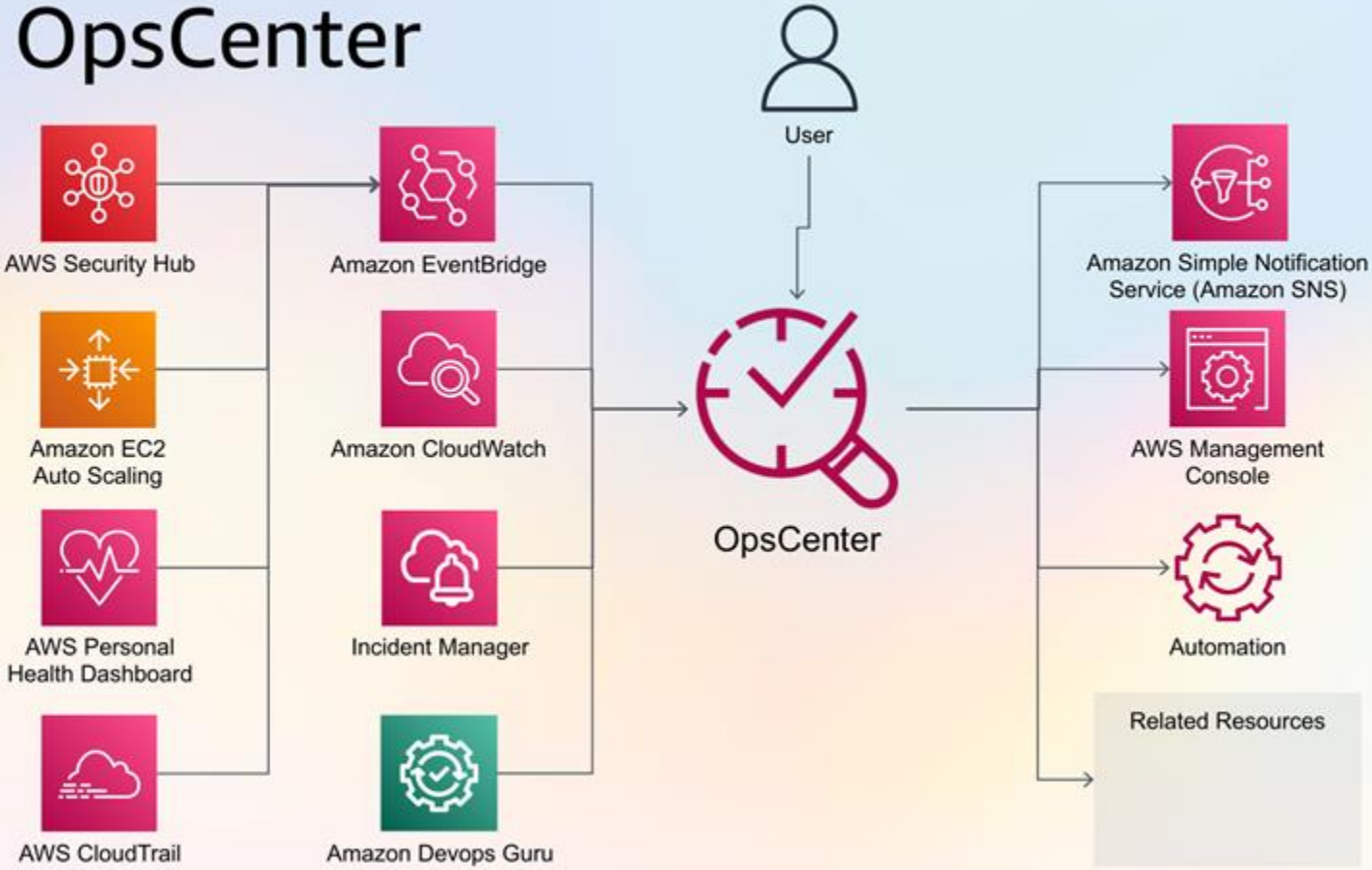
Advanced Features

PXL DIGITAL

- Use IAM permissions to control access
- Port forwarding + SSH (and SCP)
- Logging and auditing
  - CloudTrail
  - S3
  - CloudWatch Logs
  - EventBridge (based on CloudTrail)

cloudar

OpsCenter


User
AWS Security Hub
Amazon EventBridge
Amazon Simple Notification Service (Amazon SNS)
Amazon EC2 Auto Scaling
Amazon CloudWatch
AWS Management Console
OpsCenter
AWS Personal Health Dashboard
Incident Manager
Automation
Related Resources
AWS CloudTrail
Amazon Devops Guru

OpsCenter

Centrally diagnose and remediate issues with dashboards

Use Cases

- Remediate Operational Issues
  - Security or Performance Issues
  - Failures and AWS Health alerts
  - Resource State Changes
- Monitor Patch Compliance
- Review instance count and AMI usage

Key Features

- Gain insight into operations issues
- View operations data across AWS accounts/Regions
- Aggregates information from native AWS services
- (AWS Config, AWS CloudTrail, Amazon CloudWatch Events, etc.)

AWS Systems Manager

PXL DIGITAL

- Operations Management
  - Explorer
  - **OpsCenter**
  - Incident Manager
- Application Management
  - Application Manager
  - AppConfig
  - **Parameter Store**
- Change Management
  - Change Manager
  - **Automation**
  - Maintenance Windows
- Node Management
  - Fleet Manager
  - Compliance
  - Inventory
  - **Session Manager**
  - Run Command
  - State Manager
  - Patch Manager
  - Distributor

cloudar

Parameter Store

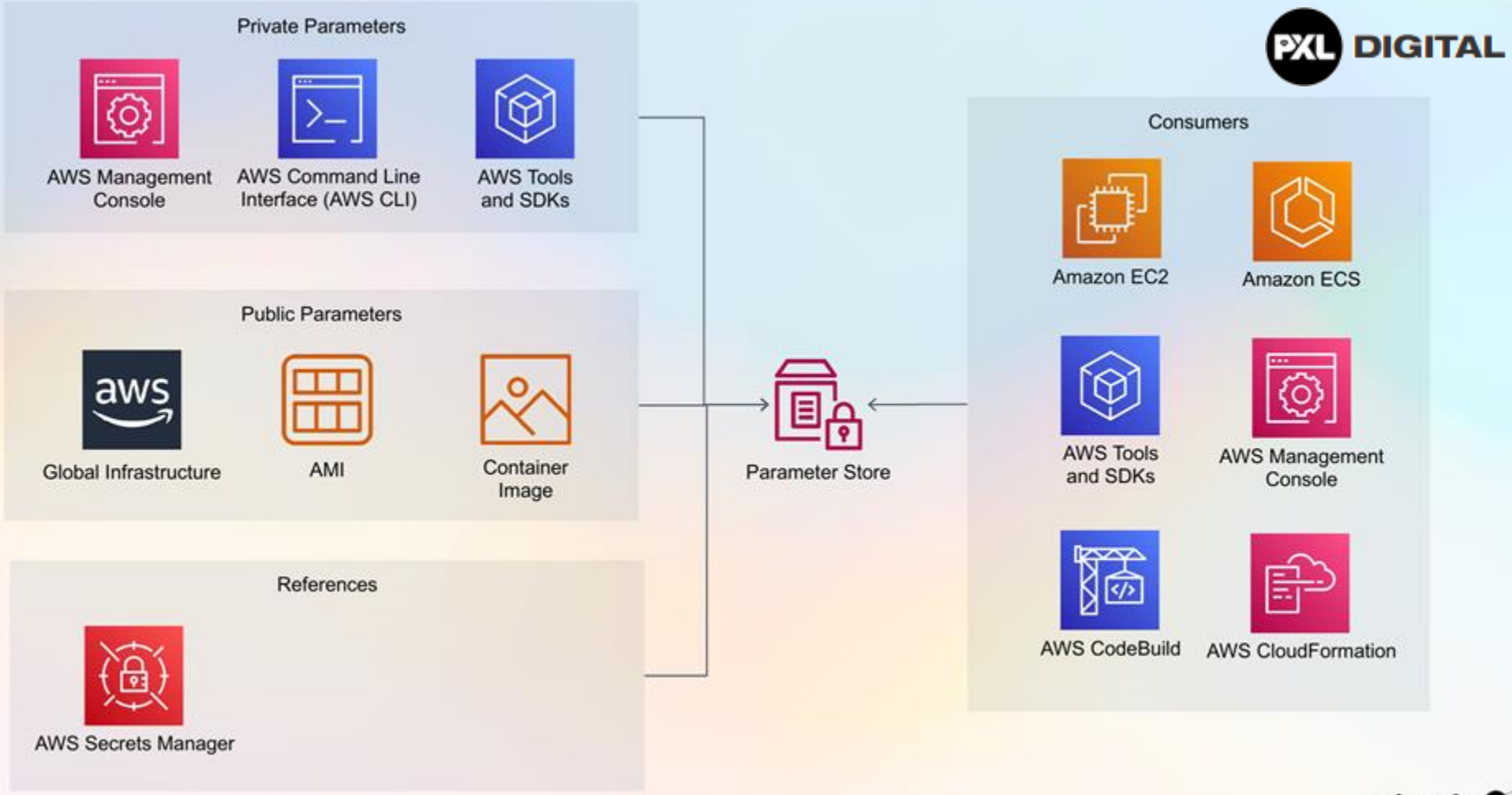
Secure, hierarchical storage for configuration data management and secrets management

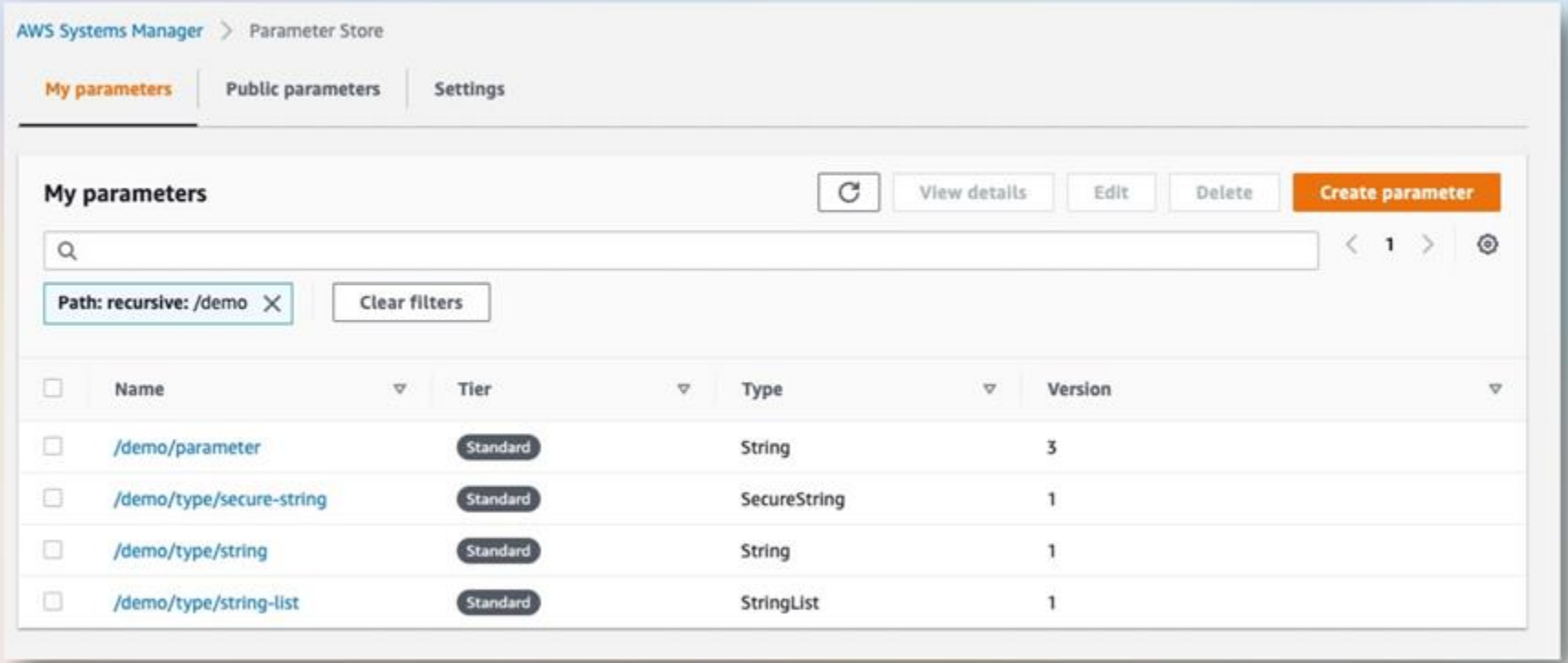
Use Cases

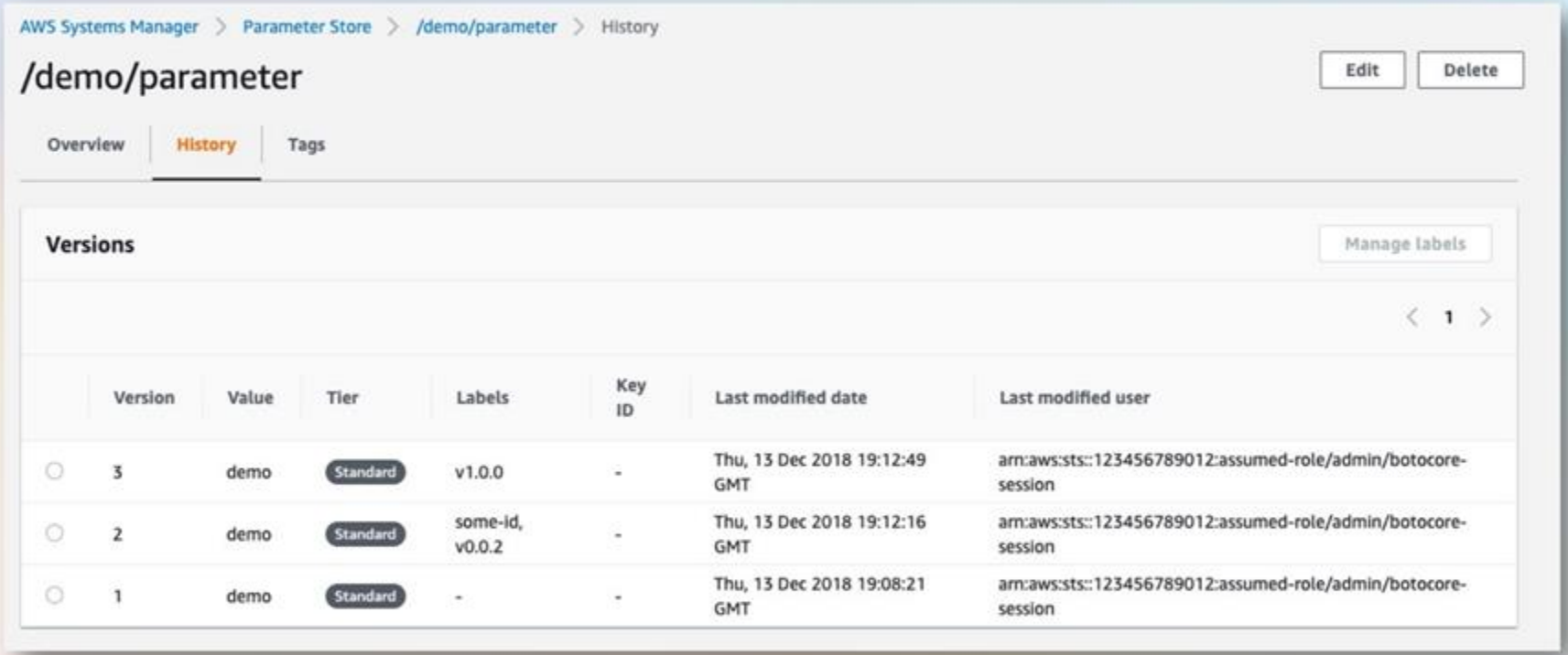
- centralized way to manage configuration data.
- store different logins and reference streams.
- receive notifications when secrets and passwords are or aren't changed.

Key Features

- Change notification
- Organize and control access
- Label versions
- Data validation
- Reference secrets
- Accessible from other AWS services
- Integrate with other AWS services


Private Parameters
AWS Management Console
AWS Command Line Interface (AWS CLI)
AWS Tools and SDKs
Public Parameters
Global Infrastructure
AMI
Container Image
References
AWS Secrets Manager
Parameter Store
Consumers
Amazon EC2
Amazon ECS
AWS Tools and SDKs
AWS Management Console
AWS CodeBuild
AWS CloudFormation


AWS Systems Manager
Parameter Store
My parameters
Public parameters
Settings
My parameters
View details
Edit
Delete
Create parameter
1
Path: recursive: /demo
Clear filters
Name
Tier
Type
Version
/demo/parameter
Standard
String
3
/demo/type/secure-string
Standard
SecureString
1
/demo/type/string
Standard
String
1
/demo/type/string-list
Standard
StringList
1



AWS Systems Manager > Parameter Store > /demo/parameter > History

/demo/parameter

Edit Delete

Overview | History | Tags

Versions

Manage labels

< 1 >

	Version	Value	Tier	Labels	Key ID	Last modified date	Last modified user
○	3	demo	Standard	v1.0.0	-	Thu, 13 Dec 2018 19:12:49 GMT	arn:aws:sts::123456789012:assumed-role/admin/botocore-session
○	2	demo	Standard	some-id, v0.0.2	-	Thu, 13 Dec 2018 19:12:16 GMT	arn:aws:sts::123456789012:assumed-role/admin/botocore-session
○	1	demo	Standard	-	-	Thu, 13 Dec 2018 19:08:21 GMT	arn:aws:sts::123456789012:assumed-role/admin/botocore-session

Advanced Features

PXL DIGITAL

- Change notifications (EventBridge)
- Standard and Advanced Tier
- Parameter Policies (expiration, no-change notification)

	Standard	Advanced
Total number of parameters allowed (per AWS account and AWS Region)	10,000	100,000
Maximum size of a parameter value	4 KB	8 KB
Parameter policies available	No	Yes For more information, see Assigning parameter policies.
Cost	No additional charge	Charges apply For more information, see AWS Systems Manager Pricing.

cloudar

AWS Systems Manager

PXL DIGITAL

- Operations Management
  - Explorer
  - **OpsCenter**
  - Incident Manager
- Application Management
  - Application Manager
  - AppConfig
  - **Parameter Store**
- Change Management
  - Change Manager
  - **Automation**
  - Maintenance Windows
- Node Management
  - Fleet Manager
  - Compliance
  - Inventory
  - **Session Manager**
  - Run Command
  - State Manager
  - Patch Manager
  - Distributor

cloudar

Automation

PXL DIGITAL

Simplifies common maintenance, deployment, and remediation tasks for AWS services

Use Cases

- One-click configuration tasks
- Performing routine maintenance tasks
- Automatic remediation through AWS Config
- Stopping EC2 instances with approvals
- Taking backups of AWS resources (e.g. DynamoDB)

Key Features

- Scripting support in runbook content
- Run automations from a centralized location
- Enhanced operations security
- Safely perform disruptive tasks in bulk
- Define constraints for inputs
- Log automation action output to Amazon CloudWatch Logs
- Share organizational best practices

How does Automation work?

PXL DIGITAL

- Assumes current user context by default
- Option to specify service role
- Leverage AWS provided playbooks
- Create custom Automation documents
  - Define actions to perform
  - Provide dynamic parameters
  - Conditionally branch based on step results
  - Configure approvals as part of workflow

- Run the Automation playbook
  - Multi-account and multi-Region
  - Register as a Maintenance Window task
  - Remediation with OpsCenter
  - Trigger based on CloudWatch Event rules
  - Automatic remediation with AWS Config

Runbooks (aka Automation Documents)

Actions:

- Flow control
- Call AWS APIs and wait for properties
- Interact with Instances, AMIs and CloudFormation Stacks
- Run Automations or Commands
- Execute Lambda Functions or Step Functions
- Execute scripts (python or powershell)

Advanced usages

- Trigger based on events
  - EventBridge
  - State Manager
  - Maintenance Window
- Target groups of instances
- Use rate controls
- Run across regions and accounts

Extra leermaterialen & labs

- **Lab:** https://cloudexpert.dubbadub.be/#/2_system
- https://docs.aws.amazon.com/systems-manager/
- Bronvermelding slides:
- Ben Bridts (Cloudar): https://speakerdeck.com/benbridts/aws-systems-manager
- AWS Techtalk: https://pages.awscloud.com/AWS-Systems-Manager-Gain-Operational-Insights-and-Take-Action-on-AWS-Resources_2020_0220-MGT_OD.html