Capabilities

Patching and Patch Management

A key security control for Enterprise organizations is ensuring their fleet of cloud based operating systems maintain current patch levels. While the Enterprise probably has robust policies and capabilities in place for on premise patching, several cloud use-cases can challenge the assumptions those systems were built to solve:

- **Isolated networking**: A common design pattern for cloud deployments is to fully isolate certain environments in their own private network. Without network connectivity to corporate systems, traditional capabilities for pushing patches will often be ineffective.

- **Auto-scaling and on-demand servers**: One huge advantage of cloud is the ability to rapidly scale up and scale down computing resources to meet the workload demands of your application. This often creates challenges to standard practices of inventory management and patching at the enterprise level.

- **Capability Leapfrog**: Too often on premise OS management and patching relies on manual work from managed service providers. Many Enterprises moving to the cloud are looking to automate these activities to achieve greater scalability, control and visibility to their security posture.

**Turbot Advantage**

Turbot provides a consistent hierarchal model to automate implementation and configuration of Amazon Systems Manager across all AWS accounts used by the enterprise. Through this automation, Turbot enables inventory collection and patch management of your cloud environment, even when the instances are fully isolated from a networking perspective.
Targeting of Instances

Turbot uses specially named tags to target instances for inventory collection and selection of maintenance windows.

- Inventory collection enabled by the setting the instance tag
  - Tag Key: `turbot:InventoryCollection`
  - Tag Value: `true`

- Patching is enabled by setting the instance tag:
  - Tag Key: `turbot:PatchingMaintenanceWindow`
  - Tag Value: `<Name of Maintenance Window>`

- The Patch Baseline is chosen via the optional SSM Patch Group tag
  - Tag Key: `Patch Group`
  - Tag Value: `<Name of Patch Baseline>`
  - Default: If not set the instance will be associated with the “Default” patch baseline.

SSM Specific Tagging Guardrails

**AWS > SSM > Instance Patch Management**

*Enforce: Enabled with Target Patch Group*

Set ‘`turbot:PatchingMaintenanceWindow`’ and ‘Patch Group’ tags for an instance based on the value of ‘AWS > EC2 > Instance Patching Maintenance Window’ and ‘AWS > EC2 > Instance Target Patch Group’

**AWS > EC2 > Instance Approved Patch Groups**

*YAML List*

A list of patch group names that are approved for use.

**AWS > EC2 > Instance Target Patch Group**

*Text Value*

The patch group name that will be enforced as the Target patch group, or used as the initial patch group if enforcing with approved patch group. Must be part of the approved patch group list to be valid.

**AWS > EC2 > Instance Patching Maintenance Window**

*Text Value*

Set the maintenance window to be used for automatic patching. To be valid the `Selected maintenance window must be defined in the policy SSM > Maintenance Window Definitions`
AWS > EC2 > Instance Target Patch Group

**Text Value**
*The patch group name that will be enforced as the Target patch group, or used as the initial patch group if enforcing with approved patch group. Must be part of the approved patch group list to be valid.*

AWS > EC2 > Inventory Collection for Bob's Demo Account

**Enforce: Inventory collection enabled**
*Apply the turbot:InventoryCollection tag to the instance and set the value to true.*

**Turbot Tagging Guardrails (optional):**
Alternatively, you can use Turbot tagging guardrails to set tags on instances based on Account or instance level metadata. Please see /help/guides/tag-management/ on your turbot installation for detailed description of Turbot tagging automation templates.

**Patch Management Template Examples**

Only do inventory collection on QA and Production accounts:

- `turbot:InventoryCollection: "{% if TagsMap['Environment'] in ['QA','Prod'] %}true{% else %}false{% endif %}"`

Setting different patch maintenance windows for different environments:

- `turbot:PatchingMaintenanceWindow: "{% if TagsMap['Environment'] in ['QA','Prod'] %}MonthlyPatchWindow{% else %}WeeklyPatchWindow{% endif %}"`
Systems Manager Setup

Instance Roles & Profiles

By default, Systems Manager doesn't have permission to perform actions on your instances. You must enable access by creating an IAM instance profile role. Turbot has guardrails to automate this process for you:

Policies – Instance Roles Profiles & Policies

AWS > IAM > EC2 Role Has Turbot Default Instance Policies

**Enforce: Attach Turbot default instance policies**

*Check that any role which can be attached to an EC2 instance has the Turbot EC2 Instance default policy attached to it. This allows dev teams to use their own instance profiles, but ensures that minimum access needed for SSM exists.*

AWS > IAM > Turbot EC2 Instance Role

**Enforce: Manage role**

*Set whether Turbot should check if the Turbot EC2 instance role is configured correctly. Allows for override of default behavior for specific account or instance level exceptions.*

AWS > IAM > Turbot Maintenance Window Role

**Enforce: Manage role**

*Determines if Turbot should check that the Turbot maintenance window role is configured correctly.*

AWS > EC2 > Instance Has Default EC2 Instance Profile Attached

**Enforce: Attach default EC2 instance profile if no instance profile is attached**

*Check if an EC2 instance has the default EC2 instance profile attached (as specified by EC2:DefaultEC2InstanceProfileName).*

AWS > EC2 > Default EC2 Instance Profile Name

**Text Value**

*The name of the default instance profile to attached to EC2 instances. To use the Turbot managed default role, set to ec2_instance_default.*

AWS > SSM > Turbot EC2 Instance Role Permissions

**Enabled if SSM > App Enabled**

*Include SSM permissions in Turbot default EC2 instance role permissions.*
Install SSM Agent
Amazon Linux and AWS Windows AMIs have the Amazon SSM agent preinstalled. For other Linux OSs, Turbot provides an automation (using an Ansible guardrail to install the SSM agent on those platforms).

Policies – SSM Agent

Linux > Install SSM Agent

**Enabled**

*Install the SSM agent on instances launched with the Turbot key pair. This will allow the instance to be managed by SSM.*

SSM User Permissions and access
Your operation teams managing patching or your application teams (if patching is managed by the app teams) will need permissions to SSM to configure maintenance windows and view reports.

Policies – SSM Whitelisting

AWS> SSM > App Enabled

**Enabled**

*Enables SSM in the Service Whitelist.*

AWS> SSM > Rights

**Enforce: Enabled if SSM > App Enabled**

*Enables SSM Rights (allows owners to grant AWS/SSM level rights to Turbot users).*
SSM Maintenance Windows

Overview
By specifying maintenance windows in Turbot, Turbot will both ensure that the specified maintenance window is configured in AWS SSM and that the maintenance window selected at the instance level is one of the approved maintenance windows.

Policies – Maintenance Window Configuration
Maintenance windows are defined with one policy and enforced with another.

AWS > SSM > Turbot Maintenance Window Definitions

YAML Template

*Definition of the Turbot maintenance windows. Example:*

- Name: Every8Hours
  Description: 'Turbot Every 8 Hours Maintenance Window'
  Schedule: 'cron(0 0 */8 * * ? *)'
  Duration: 4
  Cutoff: 1
  AllowUnassociatedTargets: false

- Name: Every30Mins
  Description: 'Turbot Every 30 mins Maintenance Window'
  Schedule: 'rate(30 minutes)'
  Duration: 1
  Cutoff: 0
  AllowUnassociatedTargets: false

- Name: Daily
  Description: 'Turbot Daily Maintenance Window'
  Schedule: 'cron(0 0 22 ? * *)'
  Duration: 4
  Cutoff: 1
  AllowUnassociatedTargets: false

- Name: Weekly
  Description: 'Turbot Weekly Maintenance Window'
  Schedule: 'cron(0 0 22 ? * MON *)'
  Duration: 4
  Cutoff: 1
  AllowUnassociatedTargets: false

AWS > EC2 > Instance Patching Maintenance Window

Text Value

*Set the maintenance window to be used for automatic patching. To be valid the Selected maintenance window must be defined in the policy SSM > Maintenance Window Definitions*

AWS > EC2 > Turbot Maintenance Windows

Enforce: Manage Turbot maintenance windows

*Set whether Turbot should check if the Turbot maintenance windows are configured correctly.*
Enabling Patch Management Feature in Turbot

Patch management is released as a Preview feature in Turbot (version 2.4). While in the preview stage, customers will have to specifically enable the feature by enabling the feature flag Parameter in the Turbot-Console CloudFormation script.

To do this a cloud admin (with appropriate permissions) will need to login to the Turbot Master AWS account, navigate to the CloudFormation and select the current Turbot-Console CF script and choose Actions > Update Stack.

On the Parameter configuration page, add “PatchManagement” to the list of flags enabled. (Add the flag without quotes and make sure to use commas to delimit the flag from other flags that may be enabled.

Continue the update of the stack (just like a standard Turbot update process). When the script runs, Turbot will start a rolling update of your cluster, at the end of that process, the feature and associated options will be enabled in your cluster. (Please note, due to browser caching, you may need to do a hard refresh of Turbot in your browser window for the new options to appear.)

Patching Configuration in Turbot

Turbot recommends creating a default patching resource group that creates common patching requirements, and attaching that to the cluster level. This will ensure that new accounts adopt a baseline patching standard from the start.

Specific resource groups for common patching design patterns can then be created and set at the account level or the instance level:

- Production Accounts (Monthly)
- Non-Prod Accounts (Weekly)
- No Patch / Manual Patching
About Turbot

Our mission at Turbot is to unlock the value of public cloud for enterprises through innovation, insight and speed. Turbot has built a strong brand and reputation by hiring the right people, continually innovating and enhancing the product, and providing unparalleled customer service.

Contact Us

Email: info@turbot.com
Twitter: @turbothq
LinkedIn: https://www.linkedin.com/company/turbot
Phone: +1 973 922 0297
Address: https://turbot.com

Turbot HQ, Inc
1732 1st Ave #20232
New York, NY 10128 USA